User Interface Description

English

# PRIMERGY BX600 Blade Server Systems

## Intelligent Blade Panel Module 30/12

# PRIMERGY BX600 Blade Server Systems

Intelligent Blade Panel Module 30/12

Edition March 2008

## Comments… Suggestions… Corrections…

The User Documentation Department would like to know your opinion on this manual. Your feedback helps us to optimize our documentation to suit your individual needs.

Feel free to send us your comments by e-mail to:
manuals@fujtsu-siemens.com

## Certified documentation according to DIN EN ISO 9001:2000

To ensure a consistently high quality standard and user-friendliness, this documentation was created to meet the regulations of a quality management system which complies with the requirements of the standard DIN EN ISO 9001:2000.

cognitas. Gesellschaft für Technik-Dokumentation mbH
www.cognitas.de

## Copyright and Trademarks

Copyright © Fujitsu Siemens Computers GmbH 2008.

All rights reserved.
Delivery subject to availability; right of technical modifications reserved.

All hardware and software names used are trademarks of their respective manufacturers.

Important Notes

Introduction

Networking Planning

Making Network Connection

Configuration the IBP

Web Base Command Interface

Command Reference

Using SNMP

System Defaulting

Troubleshooting and Tips

# CONTENTS


1 Important Notes ..... 8
1.1 Information About Boards ..... 8
1.2 Compliance Statements ..... 9
2 Introduction ..... 12
2.1 Features of the IBP Module ..... 13
2.1.1 MAC Address Supported Features ..... 13
2.1.2 Layer 2 Features ..... 14
2.1.3 IBP Module Management Features ..... 16
2.1.4 Security Feature ..... 18
2.2 Description of Hardware ..... 19
2.2.1 Ethernet Ports ..... 19
2.3 Features and Benefits ..... 23
2.4 Notational Conventions ..... 25
2.5 Target Group ..... 26
2.6 Technical Data ..... 27
3 Network Planning ..... 29
3.1 Introduction to IBP ..... 29
4 Making Network Connections ..... 30
4.1 Connecting to 1000BASE-T Devices ..... 30
4.2 1000BASE-T Cable Requirements ..... 31
4.3 1000BASE-T Pin Assignments ..... 32
5 Configuration the IBP Module ..... 33
5.1 Overview ..... 33
5.2 Connecting the IBP Module ..... 34
5.3 Start up and Configuration the IBP Module ..... 36
5.4 Configuring the Terminal ..... 37
5.5 Booting Device ..... 38
5.6 Software Download ..... 39
5.6.1 In BootROM Back Door CLI ..... 39
5.6.2 In Operation Code CLI ..... 40
6 Web-Based Management Interface ..... 43
6.1 Overview ..... 43
6.2 Main Menu ..... 44
6.2.1 Groups Administration ..... 44
6.2.2 Panel Settings Menu ..... 61
6.2.3 Security Menu ..... 90

6.2.4 Extended Configuration Menu ..... 100
7 Command Reference ..... 131
7.1 CLI Command Format ..... 131
7.2 CLI Mode-based Topology ..... 132
7.3 System Information and Statistics commands ..... 134
7.3.1 show arp ..... 134
7.3.2 show calendar ..... 134
7.3.3 show eventlog ..... 135
7.3.4 show running-config ..... 135
7.3.5 show sysinfo ..... 136
7.3.6 show system ..... 137
7.3.7 show hardware ..... 137
7.3.8 show version ..... 138
7.3.9 show loginsession ..... 139
7.4 Device Configuration Commands ..... 140
7.4.1 Interface ..... 140
7.4.2 L2 MAC Address and Multicast Forwarding Database Tables ..... 153
7.4.3 IGMP Snooping ..... 157
7.4.4 Port Channel ..... 158
7.4.5 Uplink Sets ..... 159
7.4.6 Port Group ..... 160
7.4.7 Port Backup ..... 162
7.4.8 Link State ..... 164
7.4.9 VLAN Port Groups ..... 165
7.4.10 Service LAN ..... 168
7.4.11 Service VLAN ..... 170
7.5 Management Commands ..... 172
7.5.1 Network Commands ..... 172
7.5.2 Serial Interface Commands ..... 177
7.5.3 Telnet Session Commands ..... 180
7.5.4 SNMP Server Commands ..... 186
7.5.5 SNMP Trap Commands ..... 194
7.5.6 HTTP commands ..... 197
7.5.7 Secure Shell (SSH) Commands ..... 201
7.5.8 DHCP Client Commands ..... 204
7.5.9 LOCK Commands ..... 206
7.6 System Log Management Commands ..... 208

7.6.1 Show Commands ..... 208
7.6.2 show logging buffered ..... 208
7.6.3 show logging traplog ..... 209
7.6.4 Configuration Commands ..... 210
7.7 Script Management Commands ..... 215
7.7.1 script apply ..... 215
7.7.2 script delete ..... 215
7.7.3 script list ..... 216
7.7.4 script show ..... 216
7.8 User Account Management Commands ..... 217
7.8.1 Show Commands ..... 217
7.8.2 Configuration Commands ..... 217
7.9 Security Commands ..... 220
7.9.1 Show Commands ..... 220
7.9.2 Configuration Commands ..... 231
7.9.3 Dot1x Configuration Commands ..... 234
7.9.4 Radius Configuration Commands ..... 240
7.9.5 TACACS Configuration Commands ..... 244
7.9.6 Port Security Configuration Commands ..... 248
7.10 SNTP Commands ..... 251
7.10.1 Show Commands ..... 251
7.10.2 Configuration Commands ..... 252
7.11 System Utilities ..... 257
7.11.1 clear ..... 257
7.11.2 copy ..... 263
7.11.3 delete ..... 266
7.11.4 dir ..... 266
7.11.5 whichboot ..... 267
7.11.6 boot-system ..... 267
7.11.7 ping ..... 268
7.11.8 traceroute ..... 269
7.11.9 logging cli-command ..... 270
7.11.10 calendar set ..... 270
7.11.11 reload ..... 271
7.11.12 configure ..... 271
7.11.13 disconnect ..... 271
7.11.14 hostname ..... 272

7.11.15 quit ..... 272
7.12 DHCP Commands ..... 273
7.12.1 ip dhcp restart ..... 273
7.12.2 ip dhcp client-identifier ..... 273
8 Using SNMP ..... 274
8.1 Supported MIBs ..... 275
8.2 Accessing MIB Objects ..... 277
8.3 Supported Traps ..... 280
9 Default Settings ..... 281
9.1 The overview system default settings ..... 281
9.2 The default settings for all the configuration commands ..... 282
10 Troubleshooting and Tips ..... 286
10.1 Diagnosing IBP Indicators ..... 286
10.2 Accessing the Management Interface ..... 287

# 1 Important Notes

Store this manual close to the device. If you pass the device on to third parties, you should pass this manual on with it.

Be sure to read this page carefully and note the information before you open the device.

You cannot access the IBP Module without first opening the device. How to dismantle and reassemble the device is described in the Operating Manual accompanying the device.

Please observe the safety information provided in the “Important Notes” chapter in the device’s operating manual.

Components can become very hot during operation. Ensure you do not touch components when handling the device. There is a danger of burns!

The warranty is invalidated if the device is damaged during the installation.

## 1.1 Information About Boards

To prevent damage to the device or the components and conductors on it, please take great care when you insert or remove it. Take great care to ensure that the board is slotted in straight, without damaging components or conductors on it, or any other components.

Be especially careful with the locking mechanisms (catches, centering pins etc.) when you replace the board.

Never use sharp objects (screwdrivers) for leverage.

Boards with electrostatic sensitive devices (ESD) are identifiable by the label shown.

When you handle boards fitted with ESDs, you must, under all circumstances, observe the following points:

You must always discharge static build up (e.g., by touching a grounded object) before working.

The equipment and tools you use must be free of static charges.

Remove the power plug from the mains supply before inserting or removing boards containing ESDs.

- Always hold boards with ESDs by their edges.
- Never touch pins or conductors on boards fitted with ESDs.

## 1.2 Compliance Statements

**FCC Class A Compliance**

This equipment has been tested and found to comply with the limits for a “Class A” digital device, pursuant to Part 15 of the FCC rules and meets all requirements of the Canadian Interference-Causing Equipment Regulations. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in strict accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between equipment and the receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

- Consult the dealer or an experienced radio/TV technician for help.

Fujitsu Siemens Computers is not responsible for any radio or television interference caused by unauthorized modifications of this equipment or the substitution or attachment of connecting cables and equipment other than those specified by Fujitsu Siemens Computers. The correction of interferences caused by such unauthorized modification, substitution or attachment will be the responsibility of the user.

You may use unshielded twisted-pair (UTP) cables for RJ-45 connections – Category 3 or greater for 10 Mbps connections, Category 5 for 100 Mbps connections, and Category 5 or 5e for 1000 Mbps connections.

Wear an anti-static wrist strap or take other suitable measures to prevent electrostatic discharge when handling this equipment.

**Industry Canada - Class A**

This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus as set out in the interference-causing equipment standard entitled “Digital Apparatus,” ICES-003 of the Department of Communications.

Cet appareil numérique respecte les limites de bruits radioélectriques appli- cables aux appareils numériques de Classe A prescrites dans la norme sur le matériel brouilleur: “Appareils Numériques,” NMB-003 édictée par le ministère des Communications.

### Japan VCCI Class A

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

### CE Mark Declaration of Conformance for EMI and Safety (EEC)

This information technology equipment complies with the requirements of the Council Directive 89/336/EEC on the Approximation of the laws of the Member States relating to Electromagnetic Compatibility and 73/23/EEC for electrical equipment used within certain voltage limits and the Amendment Directive

93/68/EEC. For the evaluation of the compliance with these Directives, the following standards were applied:

RFI Emission:
- Limit class A according to EN 55022:1998
- Limit class A for harmonic current emission according to EN 61000-3-2/1995
- Limitation of voltage fluctuation and flicker in low-voltage supply system according to EN 61000-3-3/1995

Immunity:
- Product family standard according to EN 55024:1998
- Electrostatic Discharge according to EN 61000-4-2:1995 (Contact Discharge: ±4 kV, Air Discharge: ±8 kV)
- Radio-frequency electromagnetic field according to EN 61000-4-3:1996 (80 - 1000 MHz with 1 kHz AM 80% Modulation: 3 V/m)
- Electrical fast transient/burst according to EN 61000-4-4:1995 (AC/DC power supply: ±1 kV, Data/Signal lines: ±0.5 kV)
- Surge immunity test according to EN 61000-4-5:1995 (AC/DC Line to Line: ±1 kV, AC/DC Line to Earth: ±2 kV)
- Immunity to conducted disturbances, Induced by radio-frequency fields: EN 61000-4-6:1996 (0.15 - 80 MHz with 1 kHz AM 80% Modulation: 3 V/m)
- Power frequency magnetic field immunity test according to EN 61000-4-8:1993 (1 A/m at frequency 50 Hz)
- Voltage dips, short interruptions and voltage variations immunity test according to EN 61000-4-11:1994 (>95% Reduction @10 ms, 30% Reduction @500 ms, >95% Reduction @5000 ms)

LVD:
- EN 60950 (A1/1992; A2/1993; A3/1993; A4/1995; A11/1997)

Do not plug a phone jack connector in the RJ-45 port. This may damage this device. Les raccordeurs ne sont pas utilisé pour le système télépho- nique!

**Taiwan BSMI Class A**

警告使用者：這是甲類的資訊產品，在居住的
環境中使用時，可能會造成射頻干擾，在這種
情況下，使用者會被要求採取某些適當的對策。

**Australia AS/NZS 3548 (1995) - Class A**

# 2 Introduction

The PRIMERGY BX600 Blade Server system is a modular server system that can integrates up to 10 server modules, four IBP Modules (one IBP will be included in the base enclosure, the other three are optional) and two Management Modules (MMB). The IBP Module provides networking connectivity to PRIMERGY BX600 Blade Server. The Management Modules provides a single point of control for the PRIMERGY BX600 Blade Server.

The PRIMERGY BX600 Intellignent Blade Panel (IBP) Modules are 42-port devices that are connected to servers through the mid-plane connectors located on PRIMERGY BX600 Blade Server middle plane. The device has 42 ports. The ports numeration starts from the internal ports g1-g30 connected to server blades, and ports g31-g42 are the external ports connecting the IBP Module to the network through the internal ports.

• 12 external RJ-45 connectors for 10/100/1000 Base-T copper ports (uplinks).
• 30 internal ports connected to servers through PRIMERGY BX600 Blade Server mid-plane connector of a VHDM type.

The terminal connection to the device is provided through the MMB board only. No access point is provided on the IBP Module front panel. For debugging and management purposes, a UART bus of each IBP Module is connected to the MMB board. The MMB board can select for management only one IBP at a time.

The IBP Module receives a power supply (12 V dc) through the mid-plane connector. A four system LED indicates the IBP Module status (Power module,MMB-selected or not).

The following figure illustrates the PRIMERGY BX600:

**Figure 1-1. PRIMERGY BX600 IBP Module Front Panel**

## 2.1 Features of the IBP Module

The IBP provides a wide range of advanced performance-enhancing features. Multicast filtering provides support for real-time network applications. Flow control eliminates the loss of packets due to bottlenecks caused by port saturation. And broadcast storm suppression prevents broadcast traffic storms from engulfing the network. Some of the management features are briefly described below.

**Head of Line Blocking**
Head of Line (HOL) blocking results in traffic delays and frame loss caused by traffic competing for the same egress port resources. HOL blocking queues packets, and the packets at the head of the queue are forwarded before packets at the end of the queue.

**Flow Control Support (IEEE 802.3X)**
Flow control enables lower speed devices to communicate with higher speed devices, by requesting that the higher speed device refrains from sending packets. Transmissions are temporarily halted to prevent buffer overflows.

**Back Pressure Support**
On half-duplex links, the receiving port prevents buffer overflows by occupying the link so that it is unavailable for additional traffic.

**Jumbo Frames Support**
Jumbo frames are frames with an MTU size of up to 9K bytes, and better utilize the network by transporting the same data using less frames. The main benefits of this facility are reduced transmission overhead, and reduced host processing overhead. Less frames leads to less I/O interrupts. This facility is typically used for server-to-server transfers.

**MDI/MDIX Support**
The IBP Module automatically detects whether the cable connected to an RJ-45 port is crossed or straight through. Standard wiring for end stations is Media-Dependent Interface (MDI) and the standard wiring for hubs and switches is known as Media-Dependent Interface with Crossover (MDIX).

**Auto Negotiation**
Auto negotiation allows an IBP Module to advertise modes of operation. The auto negotiation function provides the means to exchange information between two devices that share a point-to-point link segment, and to automatically configure both devices to take maximum advantage of their transmission capabilities.

### 2.1.1 MAC Address Supported Features

**MAC Address Capacity Support**
The IBP Module supports up to 16K MAC addresses. The IBP Module reserves specific MAC addresses for system use.

**Static MAC Entries**
MAC entries can be manually entered in the Bridging Table, as an alternative to learning them

from incoming frames. These user-defined entries are not subject to aging, and are preserved across resets and reboots.

**Self-Learning MAC Addresses**
The IBP Module enables automatic MAC address learning from incoming packets. The MAC addresses are stored in the Bridging Table.

**Automatic Aging for MAC Addresses**
MAC addresses from which no traffic is received for a given period are aged out. This prevents the Bridging Table from overflowing.

**Port Security**
Port security prevents unauthorized users from accessing your network. It allows each port to learn, or be assigned, a list of MAC addresses for devices authorized to access the network through that port. Any packet received on the port must have a source address that appears in the authorized list, otherwise it will be dropped. Port security is disabled on all ports by default, but can be enabled on a per-port basis.

**MAC Multicast Support**
Multicast service is a limited broadcast service, which allows one-to-many and many-to-many connections for information distribution. Layer 2 Multicast service is where a single frame is addressed to a specific Multicast address, from where copies of the frame are transmitted to the relevant ports.

### 2.1.2 Layer 2 Features

**IGMP Snooping**
IGMP Snooping examines IGMP frame contents, when they are forwarded by the IBP Module from work stations to an upstream Multicast router. From the frame, the IBP Module identifies work stations configured for Multicast sessions, and which Multicast routers are sending Multicast frames.

**Broadcast Storm Control**
Storm Control enables limiting the amount of Multicast and Broadcast frames accepted and forwarded by the IBP Module. When Layer 2 frames are forwarded, Broadcast and Multicast frames are flooded to all ports on the relevant VLAN. This occupies bandwidth, and loads all nodes connected on all ports.

**VLAN Transparency Supported Features**
The IBP supports VLAN transparency feature. All packets will be forwarded without any modifications as they are received.

**Link Aggregation**
One Aggregated Links may be defined, with up to 8 member ports, to form a single Link Aggregated Group (LAG). This enables:
• Fault tolerance protection from physical link disruption
• Higher bandwidth connections
• Improved bandwidth granularity
• High bandwidth server connectivity
LAG is composed of ports with the same speed, set to full-duplex operation.

**Uplink Set Support**
Uplink Sets are used to define the external connection. An “Uplink Set” is defined as a set of 1 to n external (uplink) ports, which is used in port group definitions to connect a group of server blades to the customer’s LAN. All members of a Uplink Set will form a LAG.

**Port Group Support**

Port Group feature is supported on IBP. Port Groups combine several internal ports into a group. Up to 30 groups are available for IBP. Each Port Group could be combined with a uplink set to be as its external connection. Packets only are forwarding within the same group.

**VLAN Port Group Support**

VLAN Port Group feature is used to define groups on VLAN basis, which are sharing the same Uplink Set. Up to 30 groups are available for IBP. Packets received on internal ports should be untagged packets, and the packets egress on uplink port should be tagged with the VLAN Port Group’s VLAN IDs.

Within the set of VLAN Port Groups sharing the same Uplink Set one VLAN can optionally be defined as “native VLAN”. This changes the tagging behavior at the uplink port for this native VLAN ID. Incoming untagged packets tagged with the native VLAN Id and forwarded to all the downlinks of this VLAN group. Incoming packets tagged with the native VLAN ID are dropped.

**Service VLAN & Service LAN Support**

Service VLAN & Service LAN are supported in IBP to provide dedicated ports for handling specific VLAN tagged packets. The packets with the same VLAN will be forwarded within the members. Their operations are very similar but in Service LAN, the tagged of packet egress on the uplink ports will be stripped and send as untagged packet. The members of the Service LAN & Service VLAN can be overlapped with the members of port group or VLAN Port group with different VLAN ID.

**Port Backup Support**

Port Backup feature is supported on IBP for redundant uplink ports. Two aggregation groups are created automatically as the Port Group is created. One of the aggregation groups are defined as active aggregation link, and the other is defined as backup aggregation group. As the active aggregation group is link down, the backup aggregation group will be activated for transmittion. After the active aggregation group is link up again, the backup aggregation group will be deactivated.

**Failover Propogation Support**
Blade Server has a dual-port network interface controller, and it realizes the redundant LAN ports in case of using NIC management program with LAN teaming function. In order to improve the switching time and realize the “rapid” fail-over of redundant LAN ports, Failover Propogation feature is introduced in IBP for uplink ports to speed up the switching of the redundant LAN ports.

**Link Aggregation and LACP**
LACP uses peer exchanges across links to determine, on an ongoing basis, the aggregation capability of various links, and continuously provides the maximum level of aggregation capability achievable between a given pair of systems. LACP automatically determines,

configures, binds and monitors the port binding to aggregators within the system.

**BootP and DHCP Clients**
DHCP enables additional setup parameters to be received from a network server upon system startup. DHCP service is an on-going process. DHCP is an extension to BootP. For more information on DHCP, see "Defining DHCP IP Interface Parameters".

### 2.1.3 IBP Module Management Features

The Intelligent Blade Panel can either be managed through the console port (out-of-band management) or through the network (in-band management) with SNMP, TELNET or HTTP protocols**.**

**Various Files of Management Operation:**

- There are three types of files for the Intelligent Blade Panel:
  - Configuration Files: The file stores system configuration information
  - Operation Code: Executed after system boot-up, also known as Run Time Image
  - BootRom Image: The images brought up by loader when power up. Also known as POST (Power On Self-Test)
- Due to the size of flash memory, the Intelligent Blade Panel supports only two copies for Configuration files and Operation Code respectively, but only one copy for BootRom Image**.**

**Duplication of Management file**

The Intelligent Blade Panel can copy those three types of files in three different ways.

1. Local file to local file copy: The Intelligent Blade Panel can copy an existed local Configuration File to another local file. Copy exited local Operation Code to another local file is not permitted.
2. Remote TFTP Server to Local file copy: The Intelligent Blade Panel can support to download Configuration File or Operation Code from remote server to local file.
3. Local file to remote server: The Intelligent Blade Panel can support to upload an existed local Configuration File to the remote server.
4. Running Config to local file copy
5. Running Config to remote TFTP server
6. Local file to Running Config copy
7. Remote TFTP server to Running Config copy

**Select Start-up Files**

Users can select one of two copies for Configuration Files and Operation Codes as start-up file which is used as default bootup configuration and execution image, And the other copy of Configuration File and Operation Code will be used for backup.

**Save Configuration as file**

Users can save the running configuration as a file for future use. This newly saved configuration file can be selected as start-up file later on. Or users can upload this saved configuration to the remote server for backup**.**

**Provision**

The Intelligent Blade Panel allows users to select the Configuration files to configure the system. There are two timings to configure system: Start-up and Run time.

Start-up: Select the Configuration File for start-up purpose.

Run time: Users can choose a new configuration file to reconfigure the system while system running, without rebooting the system. This function is available for CLI only.

**SNMP Alarms and Trap Logs**
The system logs events with severity codes and timestamps. Events are sent as SNMP traps to a Trap Recipient List.

**SNMP Version 1,Version 2, and Version 3**
Simple Network Management Protocol (SNMP) over the UDP/IP protocol. To control access to the system, a list of community entries is defined, each of which consists of a community string and its access privileges. There are 2 levels of SNMP security read-only and read-write.

**Web Based Management**
With web based management, the system can be managed from any web browser. The system contains an Embedded Web Server (EWS), which serves HTML pages, through which the system can be monitored and configured. The system internally converts web-based input into configuration commands, MIB variable settings and other management-related settings.

**Configuration File Download and Upload**
The IBP Module configuration is stored in a configuration file. The Configuration file includes both system wide and port specific IBP Module configuration. The system can display configuration files in the form of a collection of CLI commands, which are stored and manipulated as text files.

**TFTP Trivial File Transfer Protocol**
The IBP Module supports boot image, software and configuration upload/download via TFTP.

**Remote Monitoring**
Remote Monitoring (RMON) is an extension to SNMP, which provides comprehensive network traffic monitoring capabilities (as opposed to SNMP which allows network IBP Module management and monitoring). RMON is a standard MIB that defines current and historical MAC-layer statistics and control objects, allowing real-time information to be captured across the entire network.

**Command Line Interface**
Command Line Interface (CLI) syntax and semantics conform as much as possible to common industry practice. CLI is composed of mandatory and optional elements. The CLI interpreter provides command and keyword completion to assist user and shorten typing.

**Syslog**
Syslog is a protocol that allows event notifications to be sent to a set of remote servers, where they can be stored, examined and acted upon. Multiple mechanisms are implemented to send notification of significant events in real time, and keep a record of these events for after-the-fact usage.

**SNTP**
The Simple Network Time Protocol (SNTP) assures accurate network IBP Module clock time synchronization up to the millisecond. Time synchronization is performed by a network SNTP server. Time sources are established by Stratums. Stratums define the distance from the

reference clock. The higher the stratum (where zero is the highest), the more accurate the clock.

### 2.1.4 Security Feature

**SSL**
Secure Socket Layer (SSL) is an application-level protocol that enables secure transactions of data through privacy, authentication, and data integrity. It relies upon certificates and public and private keys. SSL version 3 and TLS version 1 are currently supported.

**Port Based Authentication (802.1x)**
Port based authentication enables authenticating system users on a per-port basis via an external server. Only authenticated and approved system users can transmit and receive data. Ports are authenticated via the Remote Authentication Dial In User Service (RADIUS) server using the Extensible Authentication Protocol (EAP).

**Locked Port Support**
Locked Port increases network security by limiting access on a specific port only to users with specific MAC addresses. These addresses are either manually defined or learned on that port. When a frame is seen on a locked port, and the frame source MAC address is not tied to that port, the protection mechanism is invoked.

**RADIUS Client**
RADIUS is a client/server-based protocol. A RADIUS server maintains a user database, which contains per-user authentication information, such as user name, password and accounting information. For more information, see "Configuring RADIUS Global Parameters".

**SSH**
Secure Shell (SSH) is a protocol that provides a secure, remote connection to an IBP Module. SSH version 1 and version 2 are currently supported. The SSH server feature enables an SSH client to establish a secure, encrypted connection with a IBP Module. This connection provides functionality that is similar to an inbound telnet connection. SSH uses RSA Public Key cryptography for IBP Module connections and authentication.

**TACACS+**
TACACS+ provides centralized security for validation of users accessing the IBP Module. TACACS+ provides a centralized user management system, while still retaining consistency with RADIUS and other authentication processes.

**System LED**
There is one IBP Module system LED with dual functions, controlled by MMB for error status reporting and blade identification. Different flashing frequencies are used to indicate the different functions. There are two functions, identification and error reporting, with identification having a higher priority than error reporting.

**NOTE:** If there is an error and the identification function is activated, the LED still functions as an identification LED. The LED can only be disabled by the MMB with a 255 seconds timeout. If an error is happening, the LED for error reporting will always be flashing and cannot be turn off. The following table describes the system LED indications.



## 2.2 Description of Hardware

**IBP Module Port Configurations**
**PRIMERGY BX600 Front Panel Port Description**

The PRIMERGY BX600 IBP Module contains 12 Gigabit Ethernet ports for connecting to the network and 30 Gigabit Ethernet ports for connecting PRIMERGY BX600 Blade Server management MMB modules.

The 12 Gigabit Ethernet ports can operate at 10, 100 or 1000 Mbps. These ports support auto negotiation, duplex mode (Half or Full duplex), and flow control. The 30 Gigabit Ethernet ports that connect to server modules can only operate at 1000 Mbps, full-duplex. These 30 ports also support flow control.

The following figure illustrates the PRIMERGY BX600 IBP front panel.

**Figure 1. PRIMERGY BX600 IBP Front Panel**

### 2.2.1 Ethernet Ports

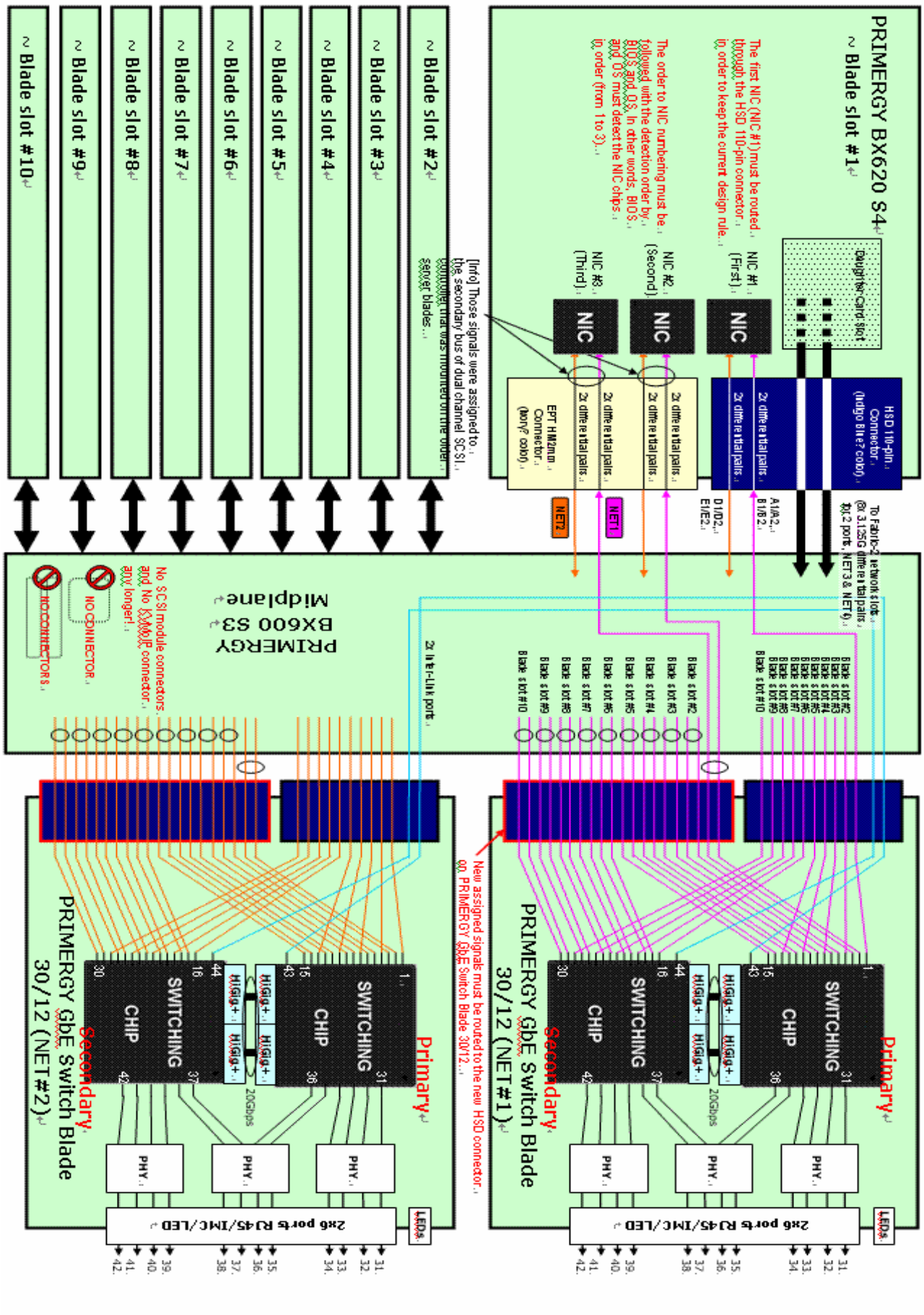
**Up-link Ports**
12 external RJ-45 ports support IEEE 802.3x auto-negotiation of speed, duplex mode, and flow control. Each port can operate at 10 Mbps, 100 Mbps and 1000 Mbps, full and half duplex, and control the data stream to prevent buffers from overflowing. The up-link ports can be connected to other IEEE 802.3ab 1000BASE-T compliant devices up to 100 m (328 ft.) away using Category 5 twisted-pair cable. These ports also feature automatic MDI/MDI-X operation, so you can use straight-through cables for all connections. These up-link ports are named g31 – g42 in the configuration interface.

**Note –** Note that when using auto-negotiation, the speed, transmission mode and flow control

can be automatically set if this feature is also supported by the attached device. Otherwise, these items can be manually configured for any connection.
**Note –** Auto-negotiation must be enabled for automatic MDI/MDI-X pin-out configuration.

### Internal Ports

The IBP also includes 30 internal 1000BASE-X Gigabit Ethernet ports that connect to the server blades in the chassis. These ports are fixed at 1000 Mbps, full duplex. The internal ports are named g1 – g30 in the configuration interface. The 30 internal ports connect with server blade as following diagram.


PRIMERGY BX620 S4
Blade slot #1
Blade slot #2
Blade slot #3
Blade slot #4
Blade slot #5
Blade slot #6
Blade slot #7
Blade slot #8
Blade slot #9
Blade slot #10
NIC
NIC
NIC
PRIMERGY BX600 S3 Midplane
PRIMERGY GbE Switch Blade 30/12 (NET#1)
PRIMERGY GbE Switch Blade 30/12 (NET#2)
Primary
Secondary
SWITCHING CHIP
PHY
2x6 ports RJ45/IMC/LED
LEDs

**PRIMERGY GbE Switch Blade 30/12 Internal Ports List**

| PRIMERGY BX620 S4 Nic No. | I/O Switch Blade Module. | Internal Ports Mapping |
|---|---|---|
| Blade No 1 Nic 1 | Net 1 | Port 1 |
| Blade No 1 Nic 2 | Net 2 | Port 1 |
| Blade No 1 Nic 3 | Net 1 | Port 2 |
| Blade No 1 Nic 4 | Net 2 | Port 2 |
| Blade No 1 Nic 5 | Net 1 | Port 3 |
| Blade No 1 Nic 6 | Net 2 | Port 3 |
| Blade No 2 Nic 1 | Net 1 | Port 4 |
| Blade No 2 Nic 2 | Net 2 | Port 4 |
| Blade No 2 Nic 3 | Net 1 | Port 5 |
| Blade No 2 Nic 4 | Net 2 | Port 5 |
| Blade No 2 Nic 5 | Net 1 | Port 6 |
| Blade No 2 Nic 6 | Net 2 | Port 6 |
| Blade No 3 Nic 1 | Net 1 | Port 7 |
| Blade No 3 Nic 2 | Net 2 | Port 7 |
| Blade No 3 Nic 3 | Net 1 | Port 8 |
| Blade No 3 Nic 4 | Net 2 | Port 8 |
| Blade No 3 Nic 5 | Net 1 | Port 9 |
| Blade No 3 Nic 6 | Net 2 | Port 9 |
| Blade No 4 Nic 1 | Net 1 | Port 10 |
| Blade No 4 Nic 2 | Net 2 | Port 10 |
| Blade No 4 Nic 3 | Net 1 | Port 11 |
| Blade No 4 Nic 4 | Net 2 | Port 11 |
| Blade No 4 Nic 5 | Net 1 | Port 12 |
| Blade No 4 Nic 6 | Net 2 | Port 12 |
| Blade No 5 Nic 1 | Net 1 | Port 13 |
| Blade No 5 Nic 2 | Net 2 | Port 13 |
| Blade No 5 Nic 3 | Net 1 | Port 14 |
| Blade No 5 Nic 4 | Net 2 | Port 14 |
| Blade No 5 Nic 5 | Net 1 | Port 15 |
| Blade No 5 Nic 6 | Net 2 | Port 15 |

| PRIMERGY BX620 S4 Nic No. | I/O Switch Blade Module. | Internal Ports Mapping |
|---|---|---|
| Blade No 6 Nic 1 | Net 1 | Port 16 |
| Blade No 6 Nic 2 | Net 2 | Port 16 |
| Blade No 6 Nic 3 | Net 1 | Port 17 |
| Blade No 6 Nic 4 | Net 2 | Port 17 |
| Blade No 6 Nic 5 | Net 1 | Port 18 |
| Blade No 6 Nic 6 | Net 2 | Port 18 |
| Blade No 7 Nic 1 | Net 1 | Port 19 |
| Blade No 7 Nic 2 | Net 2 | Port 19 |
| Blade No 7 Nic 3 | Net 1 | Port 20 |
| Blade No 7 Nic 4 | Net 2 | Port 20 |
| Blade No 7 Nic 5 | Net 1 | Port 21 |
| Blade No 7 Nic 6 | Net 2 | Port 21 |
| Blade No 8 Nic 1 | Net 1 | Port 22 |
| Blade No 8 Nic 2 | Net 2 | Port 22 |
| Blade No 8 Nic 3 | Net 1 | Port 23 |
| Blade No 8 Nic 4 | Net 2 | Port 23 |
| Blade No 8 Nic 5 | Net 1 | Port 24 |
| Blade No 8 Nic 6 | Net 2 | Port 24 |
| Blade No 9 Nic 1 | Net 1 | Port 25 |
| Blade No 9 Nic 2 | Net 2 | Port 25 |
| Blade No 9 Nic 3 | Net 1 | Port 26 |
| Blade No 9 Nic 4 | Net 2 | Port 26 |
| Blade No 9 Nic 5 | Net 1 | Port 27 |
| Blade No 9 Nic 6 | Net 2 | Port 27 |
| Blade No 10 Nic 1 | Net 1 | Port 28 |
| Blade No 10 Nic 2 | Net 2 | Port 28 |
| Blade No 10 Nic 3 | Net 1 | Port 29 |
| Blade No 10 Nic 4 | Net 2 | Port 29 |
| Blade No 10 Nic 5 | Net 1 | Port 30 |
| Blade No 10 Nic 6 | Net 2 | Port 30 |

### 2.2.2 Status of LEDs

The front panel contains light emitting diodes (LED) that indicate the status of links, and IBP diagnostics.

**Port LEDs**

Each of uplink port has two LED indicators.

**One Gbe Port LED definition:**

| LED | Color | Function |
|---|---|---|
| LED-A (Speed) | Orange | Port Link at 1000 Mbps |
| | Green | Port Link at 100 Mbps |
| | Off | Port Link at 10 Mbps |
| LED-B (Link/Activity) | Yellow | Network Link |
| | Yellow Blink | Network Activity |
| | Off | No Network Link or port disable |

**Power, Manage of LED indicator:**

| LED | Color | Function |
|---|---|---|
| TOP | Green | Power LED |
| BUTTOM | Green | Identify LED |

**System LED**

There is one IBP Module system LED with dual functions, controlled by MMB for error status reporting and blade identification. Different flashing frequencies are used to indicate the different functions. There are two functions, identification and error reporting, with identification having a higher priority than error reporting.

**NOTE:** If there is an error and the identification function is activated, the LED still functions as an identification LED. The LED can only be disabled by the MMB with a 255 seconds timeout. If an error is happening, the LED for error reporting will always be flashing and cannot be turn off. The following table describes the system LED indications.

## 2.3 Features and Benefits

### 2.3.1 Connectivity

- 30 internal Gigabit ports for easy network integration of your server cards
- 12 external 1000BASE-T Gigabit ports for uplinking to the corporate network
- Support for auto MDI/MDI-X on external ports allows any connections to be made with

straight-through cable (with auto-negotiation enabled)

- Auto-negotiation enables each port to automatically select the optimum speed (10, 100 or 1000 Mbps) and communication mode (half or full duplex) if this feature is supported by the attached device; otherwise the port can be configured manually
- IEEE 802.3ab Gigabit Ethernet compliance ensures compatibility with standards-based network cards and switches from any vendor

### 2.3.2 Performance

- Transparent bridging
- Aggregate bandwidth up to 12 Gbps
- Switching Table with 16K MAC address entries
- Filtering and forwarding at line speed
- Non-blocking switching architecture

### 2.3.3 Management

- Telnet, SNMP/RMON and Web-based interface
- Multicast Switching based on IGMP (Internet Group Management Protocol) Snooping and Multicast Filtering
- Broadcast storm suppression
- Link aggregaton
- Management access security provided with username/password, and SNMP community names

- Telnet, SNMP/RMON and Web-based interface
- Multicast Switching based on IGMP (Internet Group Management Protocol) Snooping and Multicast Filtering
- Broadcast storm suppression
- Link aggregaton
- Management access security provided with username/password, and SNMP community names



## 2.4 Notational Conventions

The meanings of the symbols and fonts used in this manual are as follows:

| | |
|---|---|
| ⚠ **CAUTION!** | Pay particular attention to texts marked with this symbol.<br>Failure to observe this warning endangers your life, destroys th system, |
| “Quotation marks” | indicate names of chapters and terms that are being emphasized |
| **I** | This symbol is followed by supplementary information, remarks and tips. |

## 2.5 Target Group

This manual is intended for those responsible for installing and configuring network connections. This manual contains all the information required to configure the IBP.

## 2.6 Technical Data

### Electrical data

| | |
|---|---|
| Operating voltage | +12 VDC @ 3 A max |
| Maximum current | 11 A max @ 3.3 VDC |

### National and international standards

| | |
|---|---|
| Product safety | IEC 60950 / EN 60950 / UL 1950, CSA 22.2 No. 950 |
| Electromagnetic compatibility<br><br>Interference emission<br>Harmonic current<br>flicker<br>Interference immunity | FCC class A<br>Industry Canada class A<br>EN60005-2 class A<br>EN60005-3<br>VCCI class A<br>AS / NZS 3548 class A<br>EN 55022<br>EN 6100-3-2 JEIDA<br>EN 61000-3-3<br>EN 55024,<br>EN 61000-4-2/3/4/5/6/8/11 |
| CE certification to EU directives: | 73/23/EEC (low voltage directive)<br>89/336/EEC (Electromagnetic Compatibility ) |

### Dimensions

| | |
|---|---|
| Length | 242 mm |
| Height | 110 mm |

## Environmental conditions

| | |
|---|---|
| Environment class 3K2<br>Environment class 2K2 | DIN IEC 721 part 3-3<br>DIN IEC 721 part 3-2 |
| Temperature:<br>– Operating (3K2)<br>– Transport (2K2) | <br>0 °C .... 50 °C<br>-40 °C .... 70 °C |
| Humidity | 10 ... 90% |

Condensation while operating must be avoided.

# 3 Network Planning

## 3.1 Introduction to IBP

The Intelligent Blade Panel Module (IBP) provides a simple Ethernet interface option for connecting the PRIMERGY BX600 Blade Server systems to the network infrastructure. The administrative effort and network skills required to connect to the network are minimized. The number and type of configuration options on the IBP are restricted to reduce the initial setup complexity and to minimize the impact on upstream networking devices.

The IBP requires basic administration tasks similar to those required to connect a single multi-linked server to the network. Connecting the Blade Center with up to ten server blades becomes as easy as connecting a single server to the network.

The default network configuration of the IBP is consists of a single, untagged Virtual Local Area Network (VLAN). All of the uplink ports in each Port Group are aggregated together into a static Link Aggregation Group (LAG, or trunk group), which is fully compatible with Cisco Ether Channel technology. This configuration eliminates the need for Spanning Tree Protocol to prevent network loops, since the uplink ports act as a single link.

The IBP provides improved network reliability. All of the uplink ports in each Port Group participates in a static LAG, so if a link fails, the existing traffic is redirected to the other links.

The IBP software permits the copper TX uplink ports to auto-negotiate the speed (10/100/1000 Mbps), duplex (full/half) and flow-control settings of each link (the default set- ting). You can also fix these port characteristics to specified values. All of the uplink ports in each Port Group must be configured to the same port characteristics.

With Network Adaptor Teaming configured on the server blade Ethernet NIC, the servers can maintain redundant links to multiple IBP within the Blade Sever chassis to provide enhanced reliability. The L2 Failover option allows the IBP to disable the server-blade ports when all of its external uplinks are inactive. This causes the Network Adaptor Teaming soft- ware to failover to the other IBP(s) in the Blade Server Chassis.

The IBP connects server boards installed inside the system to a common switch fabric, and also provides three external ports for uplinking to external IEEE 802.3ab compliant devices. For most applications, the external ports on the IBP will be connected to other switches in the network backbone.



# 4 Making Network Connections

The IBP connects server boards installed inside the system to a common switch fabric, and also provides three external ports for uplinking to external IEEE 802.3ab compliant devices. For most applications, the external ports on the IBP will be connected to other switches in the network backbone.

## 4.1 Connecting to 1000BASE-T Devices

The data ports on the IBP operate at 10 Mbps, 100 Mbps, and 1000 Mbps, full and half duplex, with support for auto-negotiation of speed, duplex mode and flow control. You can connect any data port on the IBP to any server or workstation, or uplink to a network device such as another switch or a router. The 1000BASE-T standard uses four pairs of Category 5 twisted-pair cable for connections up to a maximum length of 100 m (328 feet).

For 1000 Mbps operation, you should first test the cable installation for IEEE 802.3ab 1000BASE-T compliance. See “1000BASE-T Cable Requirements” on page 34 for more information.

1. Prepare the devices you wish to network. For 1000 Mbps operation, make sure that servers and workstations have installed 1000BASE-T network interface cards. Other network devices should have RJ-45 ports that comply with the IEEE 802.3ab 1000BASE-T standard.

2. Prepare shielded or unshielded twisted-pair cables (straight-through or crossover) with RJ-45 plugs at both ends. Use 100-ohm Category 5 (Category 5e or better is recommended) cable for 1000 Mbps Gigabit Ethernet connections.

3. Connect one end of the cable to the RJ-45 port on the other device, and the other end to any available RJ-45 port on the IBP. When inserting an RJ-45 plug, be sure the tab on the plug clicks into position to ensure that it is properly seated.

Do not plug a phone jack connector into any RJ-45 port. This may damage the IBP. Instead, use only twisted-pair cables with RJ-45 connectors that conform with FCC standards.

For 1000 Mbps operation, all four wire pairs in the cable must be connected. When auto-negotiation is enabled, the 1000BASE-T ports support the auto MDI/MDI-X feature, which means that at any operating speed (10, 100, or 1000 Mbps), either straight-through or crossover cables can be used to connect to any server, workstation, or other network device. Make sure each twisted-pair cable does not exceed

100 meters (328 feet). (Note that auto-negotiation must be enabled to support auto MDI/MDI-X.)

## 4.2 1000BASE-T Cable Requirements

All Category 5 UTP cables that are used for 100BASE-TX connections should also work for 1000BASE-T, providing that all four wire pairs are connected. However, it is recommended that for all critical connections, or any new cable installations, Category 5e (enhanced Category 5) cable should be used. The Category 5e specification includes test parameters that are only recommenda- tions for Category 5. Therefore, the first step in preparing existing Category 5 cabling for running 1000BASE-T is a simple test of the cable installation to be sure that it complies with the IEEE 802.3ab standards.

### 4.2.1 Cable Testing for Existing Category 5 Cable

Installed Category 5 cabling must pass tests for Attenuation, Near-End Crosstalk (NEXT), and Far-End Crosstalk (FEXT). This cable testing infor- mation is specified in the ANSI/TIA/EIA-TSB-67 standard. Additionally, cables must also pass test parameters for Return Loss and Equal-Level Far-End Crosstalk (ELFEXT). These tests are specified in the ANSI/TIA/EIA-TSB-95Bulletin, “The Additional Transmission Performance Guidelines for 100 Ohm 4- Pair Category 5 Cabling”.

Note that when testing your cable installation, be sure to include all patch cables between IBP and end devices.

### 4.2.2 Adjusting Existing Category 5 Cabling for 1000BASE-T

If your existing Category 5 installation does not meet one of the test parameters for 1000BASE-T, there are basically three measures that can be applied to try and correct the problem:

1. Replace any Category 5 patch cables with high-performance Category 5e cables.
2. Reduce the number of connectors used in the link.
3. Reconnect some of the connectors in the link.

## 4.3 1000BASE-T Pin Assignments

1000BASE-T ports support automatic MDI/MDI-X operation, so you can use straight-through cables for all network connections to PCs or servers, or to other switches. (Auto-negotiation must be enabled to support auto MDI/MDI-X.)

The table below shows the 1000BASE-T MDI and MDI-X port pinouts. These ports require that all four pairs of wires be connected. Note that for 1000BASE-T operation, all four pairs of wires are used for both transmit and receive.

Use 100-ohm Category 5 or 5e unshielded twisted-pair (UTP) or shielded twisted-pair (STP) cable for 1000BASE-T connections. Also be sure that the length of any twisted-pair connection does not exceed 100 meters (328 feet).

| Pin | MDI Signal Name | MDI-X Signal Name |
|---|---|---|
| 1 | Transmit Data plus (TD1+) | Transmit Data plus (TD2 +) |
| 2 | Receive Data minus (RD1-) | Receive Data minus (RD2-) |
| 3 | Transmit Data plus (TD2+) | Transmit Data plus (TD1+) |
| 4 | Transmit Data plus (TD3+) | Transmit Data plus (TD4+) |
| 5 | Receive Data minus (RD3-) | Receive Data minus (RD4-) |
| 6 | Receive Data minus (RD2-) | Receive Data minus (RD1-) |
| 7 | Transmit Data plus (TD4+) | Transmit Data plus (TD3+) |
| 8 | Receive Data minus (RD4-) | Receive Data minus (RD3-) |

# 5 Configuration the IBP Module

This section contains information about IBP unpacking, installation, and cable connections.

## 5.1 Overview

The IBP Module is inserted in the PRIMERGY BX600 Blade Server which is a modular server system that can integrates up to 10 processor blades and four IBP Modules.

**Package Contents**
While unpacking the IBP Module, ensure that the following items are included:
• The IBP Module
• Documentation CD

**Unpacking the IBP Module**
To unpack the IBP Module:

**NOTE:** Before unpacking the IBP Module, inspect the package and report any evidence of damage immediately.

**NOTE:** An ESD strap is not provided, however it is recommended to wear one for the following procedure.
1 Open the container.
2 Carefully remove the IBP Module from the container and place it on a secure and clean surface.
3 Remove all packing material.
4 Inspect the IBP Module for damage. Report any damage immediately.

**NOTE:** The illustrations in this document might differ slightly from actual Blade Panel and chassis.

## 5.2 Connecting the IBP Module

Before configuring the IBP Module, PRIMERGY BX600 Blade Server console port must be connected to the IBP Module. To connect PRIMERGY BX600 Blade Server console port to the IBP Module, perform the following:

**1. Mount the IBP Module.**
On the console monitor the MMB application displays a login screen.

The IBP Module bootup screen is displayed.

```
                    Welcome to Management Blade 1.70D


<Username>:


+-------------------------------------------------------------------------+
|                              Console Menu                               |
+-------------------------------------------------------------------------+
(1) Management Agent
(2) Emergency Management Port
(3) Console Redirection
(4) TFTP update
(5) Logout
(6) Reboot Management Blade
(7) System Information Dump
Enter selection: 5

+-------------------------------------------------------------------------+
|           Logout!!!                                                     |
+-------------------------------------------------------------------------+
ATE0
ATE0
```

**2. Enter the provide and password. The console menu is displayed**.

```
                    Welcome to Management Blade 1.70D

<Username>:root
<Password>:****

+-------------------------------------------------------------------------+
|                              Console Menu                               |
+-------------------------------------------------------------------------+
(1) Management Agent
(2) Emergency Management Port
(3) Console Redirection
(4) TFTP update
```

(5) Logout
(6) Reboot Management Blade
(7) System Information Dump
Enter selection: 3

**3. Select (3) Console Redirection. The Console Redirection Table is displayed.**

```
+-------------------------------------------------------------------------+
|            Console Redirection Table                                    |
+-------------------------------------------------------------------------+
(1) Console Redirect Server Blade
(2) Console Redirect Switch Blade
(3) Set Return Hotkey , Ctrl+(a character) : Q
Enter selection or type (0) to quit: 2
```

```
+-------------------------------------------------------------------------+
|            Console Redirect Switch Blade                                |
+-------------------------------------------------------------------------+
Enter selection or type (0) to quit: 0
```

**4. Select (2) Console Redirection Switch Blade**

```
+-------------------------------------------------------------------------+
|            Console Redirection Table                                    |
+-------------------------------------------------------------------------+
(1) Console Redirect Server Blade
(2) Console Redirect Switch Blade
(3) Set Return Hotkey , Ctrl+(a character) : Q
Enter selection or type (0) to quit: 2

+-------------------------------------------------------------------------+
|            Console Redirect Switch Blade                                |
+-------------------------------------------------------------------------+
(1) Console Redirect Switch Blade_1
Enter selection or type (0) to quit: 1
Press <Ctrl+Q> Return Console Menu
```

## 5.3 Start up and Configuration the IBP Module

It's important to understand the IBP Module architecture when configuring the IBP Module. The IBP Module has two types of ports. One type is for interfacing the IBP Module with PRIMERGY BX600 Blade Server, and the other type are regular Ethernet ports used for connecting PRIMERGY BX600 Blade Server to the network.

The IBP Module module is connected to PRIMERGY BX600 Blade Server (Management Board) MMB through 30 internal ports called the Internal Ports. The maximum link speed through the Internal Ports is 1 Gigabit per port. The port configuration ID's are g1 to g30. To connect the IBP Module to the network there are 12 PHY based ports called the External ports. The external 12 ports are 10/100/1000 Base-T Ethernet ports. The port configuration ID's are g31 to g42.

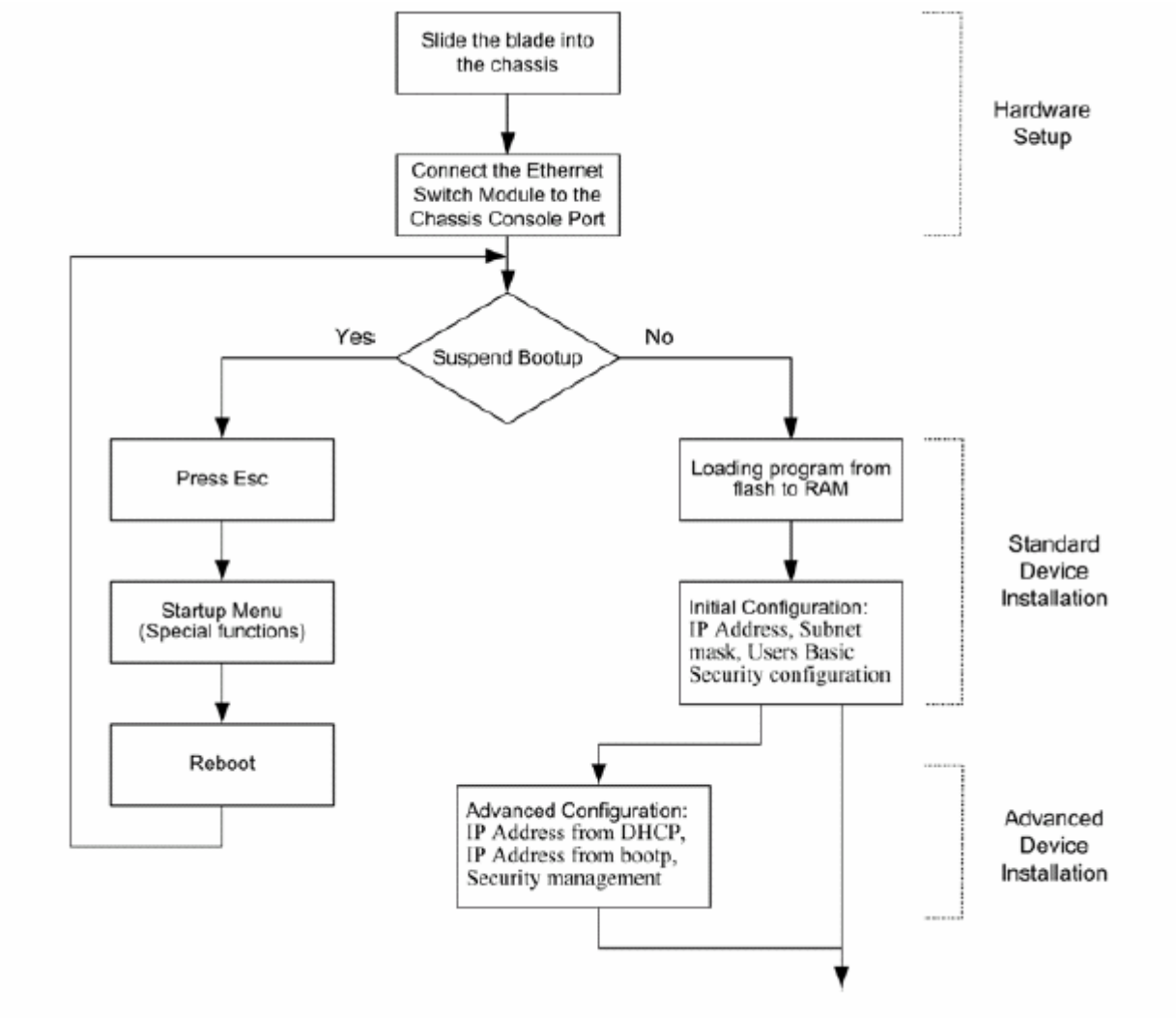
The default configuration of the internal and external ports are as follows:

**Table 4-1. Port Default Settings**

| External Ports | |
|---|---|
| **Function** | **Default Setting** |
| Flow Control | Off (disabled on ingress) |
| Back Pressure | Off (disabled on ingress) |
| Auto Negotiation | Enabled |
| Speed and duplex auto negotiation | Off (disabled on ingress) |

| Internal Ports | |
|---|---|
| **Function** | **Default Setting** |
| Speed and duplex auto negotiation | **One Gigabit / Full Speed** |
| Flow control | Enabled |
| Auto negotiation of Flow Control | Enabled |

**Figure 4-1. Installation and Configuration Flow**


Slide the blade into the chassis
Connect the Ethernet Switch Module to the Chassis Console Port
Hardware Setup
Yes
Suspend Bootup
No
Press Esc
Loading program from flash to RAM
Standard Device Installation
Startup Menu (Special functions)
Initial Configuration: IP Address, Subnet mask, Users Basic Security configuration
Reboot
Advanced Configuration: IP Address from DHCP, IP Address from bootp, Security management
Advanced Device Installation

## 5.4 Configuring the Terminal

To configure the device, the station must be running terminal emulation software. Ensure that switch module is correctly mounted and is connected to the chassis serial port. Ensure that the terminal emulation software is set as follows: Connect PRIMERGY BX600 Blade Server serial port to the IBP Module.

**NOTE:**
1. The default data rate is 9600. No other data rate is required for initial configuration.
2. Sets the data format to 9600 baudrate 9600,8 data bits, 1 stop bit, and no parity.
3. Sets Flow Control to **none**.
4. Under **Properties**, select **VT100 for Emulation** mode.
5. Select **Terminal keys** for **Function, Arrow, and Ctrl keys**. Ensure that the setting is for **Terminal keys** *(*not **Windows keys**).

For accessing IBP module from terminal perform following steps:

1. Connect your terminal to the serial port of the Chassis.

2. Power up the Chassis and observe booting information (if Chassis is running press <Enter> few times to ensure that terminal connection is successful).

## 5.5 Booting Device

• The device is delivered with a default configuration.

• The device is not configured with a default user name and password.

After connecting the PRIMERGY BX600 Blade Server serial port to the IBP Module,

When the IBP Module is connected to the local terminal, the device IBP Module goes through Power On Self Test (POST). POST runs every time the device is initialized and checks hardware components to determine if the device is fully operational before completely booting. If a critical problem is detected, the program flow stops. If POST passes successfully, a valid executable image is loaded into RAM. POST messages are displayed on the terminal and indicate test success or failure.

As the device boots, the bootup test first counts the device memory availability and then continues to boot. The following screen is an example of the displayed POST:

---------- Performing Power-On Self Tests (POST) ----------

System SDRAM Test.....…….....PASS
CPU Self Test.....…….PASS
UART Loopback Test.....……..PASS
Flash Memory Initialize.....…….PASS
Flash Memory Checksum Test.....……...PASS
PCI Bus Initialize and Test.....……PASS
System Timer Test.....……..PASS

----------Power-On Self Test Completed----------

The boot process runs approximately 60 seconds.

The auto-boot message displayed at the end of POST (see the last lines) indicates that no problems were encountered during boot. During the **BootROM Back Door Command Line Interface** can be used to run special procedures. To enter the **BootROM Back Door CLI** menu, press <Ctrl-B> within the first two seconds after the auto-boot message is displayed. If the system boot process is not interrupted by pressing <Ctrl-B>, the process continues decompressing and loading the code into RAM. The code starts running from RAM and the list of numbered system ports and their states (up or down) are displayed. After the device boots successfully, a system prompt is displayed ((vty-0) #) which is used to configure the device. However, before configuring the device, ensure that the latest software version is installed on

the device. If it is not the latest version, download and install the latest version. For more information on downloading the latest version see the "Software Download"

## 5.6 Software Download

### 5.6.1 In BootROM Back Door CLI

**Software Download Using Xmodem Protocol**
The software download procedure is performed when a new version must be downloaded to replace the corrupted files, update or upgrade the system software (system and boot images).
**NOTE: The data rate cannot be changed.**
To download software from the **BootROM CLI**:
1. From the **BootROM CLI** prompt input the following command: xmodem –rb <filename>
2. When using the HyperTerminal, click **Transfer** on the HyperTerminal Menu Bar.
3. In the **Filename** field, enter the file path for the file to be downloaded.
4. Ensure that the Xmodem protocol is selected in the **Protocol** field.
5. Press **Send**. The software is downloaded.

**Erasing the Device Configuration**
1. From the **BootROM CLI** prompt input the following command:
   *delete <configuration filename>*
   The following message is displayed:

   *Are you sure you want to delete <configuration filename> (y/n)?*

2. Press Y. The following message is displayed.
   *Updating partition table, please wait ... Done*
   *Image file <configuration filename> deleted.*
3. Repeat the device initial configuration.

**Boot Image Download**
Loading a new boot image using xmodem protocol and programming it into the flash updates the boot image. The boot image is loaded when the device is powered on. A user has no control over the boot image copies. To download a boot image using xmodem protocol:
1. Ensure that the file to be downloaded is saved on the PC host (the img file).
2. Enter `BootROM > dir -l` command to verify which software version is currently running on the device. The following is an example of the information that appears:

```
BootROM > dir -l
type       zip   def  date        version     name
-------------------------------------------------------------------------
loader     none  yes  2005/12/14  0.4         PRIMERGY BX600-l-0.4.1214.bin
bootrom    gzip  yes  2005/12/14  0.4         PRIMERGY BX600-b-0.4.1214.biz
runtime    gzip  yes  2005/01/10  0.5         PRIMERGY BX600-r-q-0.5.0110.biz

Total: 3 files.
```

3. From the **BootROM CLI** prompt input the following command: xmodem –rb <filename>
4. When using the HyperTerminal, click **Transfer** on the HyperTerminal Menu Bar.
5. In the **Filename** field, enter the file path for the file to be downloaded.
6. Ensure that the Xmodem protocol is selected in the **Protocol** field.
7. Press **Send**. The software is downloaded.

8. Enter the **reset** command. The following message is displayed:

```
BootROM > reset
Are you sure you want to reset the system (y/n)? y

System Resetting...
```

9. Enter y. The device reboots.

### 5.6.2 In Operation Code CLI

**Software Download Through TFTP Server**
This section contains instructions for downloading device software through a TFTP server. The TFTP server must be configured before beginning to download the software.

**System Image Download**
The device boots and runs when decompressing the system image from the flash memory area where a copy of the system image is stored. When a new image is downloaded, it is saved in the other area allocated for the other system image copy. On the next boot, the device will decompress and run the currently active system image unless chosen otherwise.

To download a system image through the TFTP server:

1. Ensure that an IP address is configured on one of the device ports and pings can be sent to a TFTP server.
2. Make sure that the file to be downloaded is saved on the TFTP server (the img file).
3. Enter **(vty-0) # show version** command to verify which software version is currently running on the device. The following is an example of the information that appears:

```
(vty-0) #show version
Unit1
 Serial number          :123456789
 Hardware Version       :1.0
 Number of ports        :16
 Label Revision Number  :123456789
 Part Number            :123456789
 Machine Model          :PRIMERGY BX600
 Loader version         :1.0
 Operation code version :0.50
 Boot rom version       :1.0
```

4. Enter **(vty-0) # whichboot** command to verify which system image is currently active. The following is an example of the information that appears:

```
(vty-0) #whichboot
```

```
                    file name       file type startup size (byte)
------------------------------ ------------- ------- ----------
              PRIMERGY BX600-b-0.4.1214.biz Boot-Rom image       Y       118206
                   default.cfg     Config File        Y       17336
             PRIMERGY BX600-r-c-0.5.0110.biz Operation Code       Y      40666365
```

5. Enter **(vty-0) # copy tftp://{tftp address}/{file name} image {file name}** command to copy a new system image to the device. The following message is displayed:

```
Mode..................................... TFTP
Set TFTP Server IP....................... {tftp address}
TFTP Path................................ ./
TFTP Filename............................ {file name}
Data Type................................ Code

Are you sure you want to start? (y/n)
```

6. Press Y. When the new image is downloaded, it is saved in the area allocated for the other copy of system image. The following is an example of the information that appears:

```
TFTP code transfer starting
Verifying CRC of file in Flash File System
TFTP receive complete... storing in Flash File System...
File transfer operation completed successfully.
```

7. Select the image for the next boot by entering the **boot-system** command. After this command. Enter **(vty-0) # whichboot** command to verify that the copy indicated as a parameter in the **boot-system** command is selected for the next boot. The following is an example of the information that appears:

```
(vty-0) #boot-system opcode PRIMERGY BX600-r-q-0.50.0110.biz
Start Up Success!
(vty-0) #
(vty-0) #whichboot
                    file name       file type startup size (byte)
------------------------------ ------------- ------- ----------
              PRIMERGY BX600-b-0.4.1214.biz Boot-Rom image       Y       118206
                   default.cfg     Config File        Y       17336
             PRIMERGY BX600-r-q-0.5.0110.biz Operation Code       Y      4153628
```

If the image for the next boot is not selected by entering the boot system command, the system boots from the currently active image.

8. Enter the reload command. The following message is displayed:

```
(vty-0) #reload

Are you sure you would like to reset the system? (y/n) y


System will now restart!
```

9. Enter y. The device reboots.

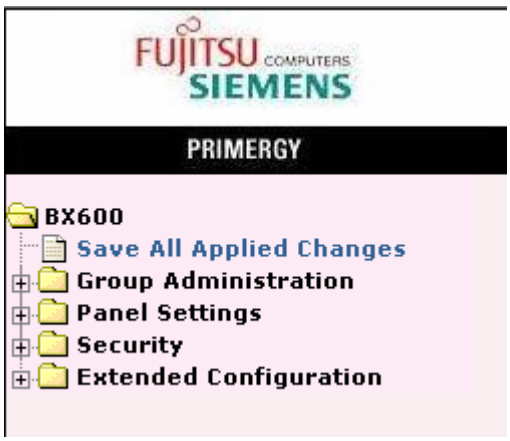
# 6 Web-Based Management Interface

## 6.1 Overview

The BX600 Network IBP module provides a built-in browser software interface that lets you configure and manage it remotely using a standard Web browser such as Microsoft Internet Explorer or Netscape Navigator. This software interface also allows for system monitoring and management of the IBP module. When you configure this IBP module for the first time from the console, you have to assign an IP address and subnet mask to the IBP module. Thereafter, you can access the IBP's Web software interface directly using your Web browser by entering the IBP's IP address into the address bar. In this way, you can use your Web browser to manage the IBP module from any remote PC station, just as if you were directly connected to the IBP's console port.

The four menu options available are: **Group Administration**, **Panel Settings**, **Security** and **Extended Configuration**.

1. **Group Administration Menu:** This section provides information for configuring Port Groups, Link State, IGMP snooping, Management VLAN and Port Backup, etc.
2. **Panel Settings Menu:** This section provides users to configure IBP interface (port), SNMP and trap manager, Ping, DHCP client, SNTP, system time, defining system parameters including telnet session and console baud rate, etc, downloading IBP module software, and resetting the IBP module.
3. **Security Menu:** This section provides users to configure IBP securities including 802.1x, Radius, TACACS, Secure Http, and Secure Shell.
4. **Extended Configuration Menu:** This section provides users to configure logging system statistics, port access control, IP filtering, and authentication.



## 6.2 Main Menu

### 6.2.1 Groups Administration

#### 6.2.1.1 Managing Uplink Sets

##### 6.2.1.1.1. Configuring Uplink Set Configuration Page

An "Uplink Set" is defined as a set of 1 to n external (uplink) ports, which is be used in port group definitions to connect a group of server blades to the customer's LAN. The purpose of the uplink set configuration is to create groups, and to add or modify the existing external ports to groups. Link state, port backup, and IGMP snooping of the uplink set groups can be configured in this page.

**Selection Criteria**

**Uplink Set Name** – Use this pull-down menu to select one of the existing uplink set.

**Configurable Data**

**Uplink Set Name** – Input the uplink set name to create a new group. It can be up to 32 alphanumeric characters, including blanks.

**Link State** – Use this pull-down menu to configure link state.

**Port Backup** – Use this pull-down menu to configure port backup

**IGMP snooping** –Use this pull-down menu to configure IGMP snooping

**Participation** –Use this field to specify whether a interface will participate in this uplink set. The factory default is 'Exclude'. The possible values are:

- Include: This interface is the member of the uplink set.
- Exclude: This interface is not the member of the uplink set.

**Non-Configurable Data**

**Slot/Port** – The interface

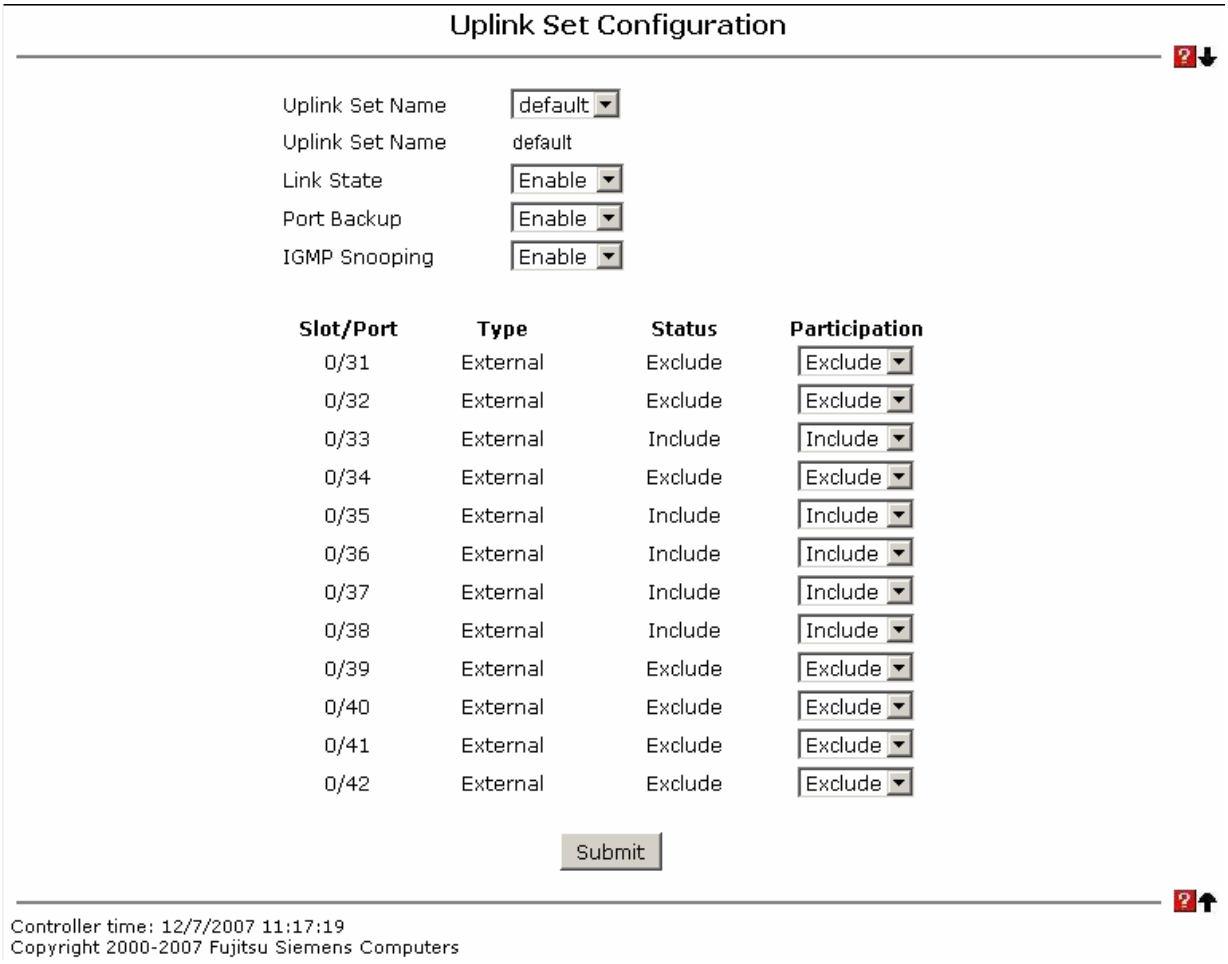
**Type** – The interface type. Type should be external.

**Status** – The interface is belong to this port group or not.

**Command Buttons**

**Submit** – Update the IBP the values on this screen. If you want the IBP to retain the new values across a power cycle, you have to perform a save

**Delete** – Delete the Uplink Set. You are not allowed to delete the "default" uplink set.




#### 6.2.1.1.2. View Uplink Set Information Page

This page displays the status of all currently configured uplink set.

**Non-Configurable Data**

**Uplink Set Name** – The group name of the uplink set.

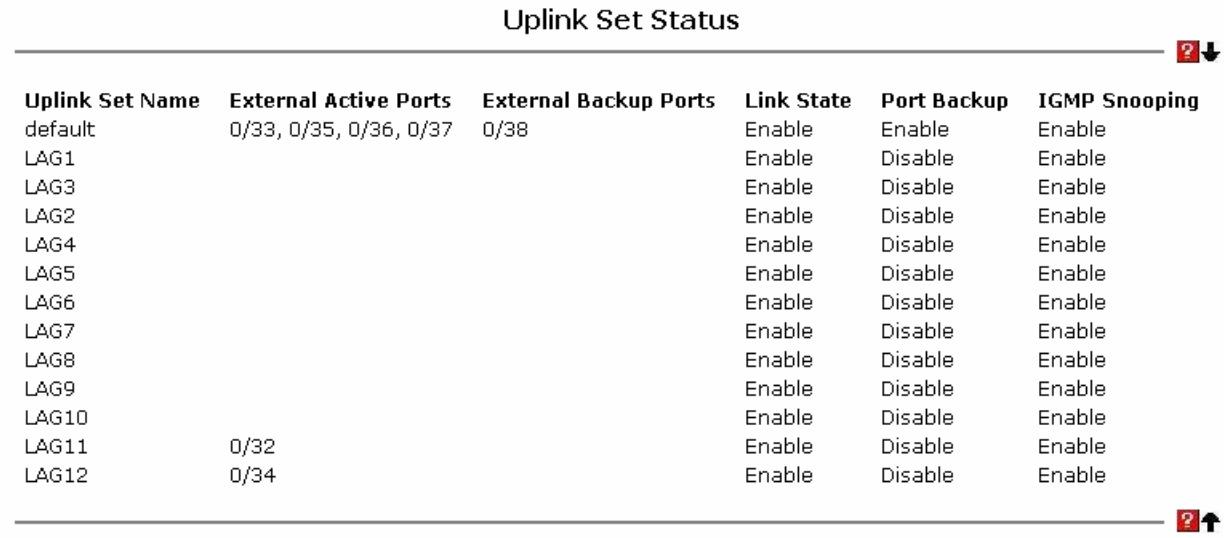
**External Active Ports** – List the external active port group members.

**External Backup Ports** – List the external backup port group members.

**Link State** – The status of the link state of that port group.

**Port Backup** - The status of the port backup of that port group.

**IGMP snooping** – The status of IGMP snooping of that port group.



Uplink Set Status

| Uplink Set Name | External Active Ports | External Backup Ports | Link State | Port Backup | IGMP Snooping |
|---|---|---|---|---|---|
| default | 0/33, 0/35, 0/36, 0/37 | 0/38 | Enable | Enable | Enable |
| LAG1 | | | Enable | Disable | Enable |
| LAG3 | | | Enable | Disable | Enable |
| LAG2 | | | Enable | Disable | Enable |
| LAG4 | | | Enable | Disable | Enable |
| LAG5 | | | Enable | Disable | Enable |
| LAG6 | | | Enable | Disable | Enable |
| LAG7 | | | Enable | Disable | Enable |
| LAG8 | | | Enable | Disable | Enable |
| LAG9 | | | Enable | Disable | Enable |
| LAG10 | | | Enable | Disable | Enable |
| LAG11 | 0/32 | | Enable | Disable | Enable |
| LAG12 | 0/34 | | Enable | Disable | Enable |

Controller time: 12/7/2007 11:22:24
Copyright 2000-2007 Fujitsu Siemens Computers

### 6.2.1.2 Managing Port Groups

#### 6.2.1.2.1. Configuring Port Group Configuration Page

The purpose of the port group configuration is to create port groups, and to modify the existing port groups. Only the internal ports could be defined to be the member of the port groups. The external connection is defined by specifying an Uplink Set.

**Selection Criteria**

**Group Name** – Use this pull-down menu to select one of the existing groups.

**Configurable Data**

**Group Name** – Input the group name to create a new port group. It can be up to 32 alphanumeric characters, including blanks.

**Uplink Set Name** – Use the pull-down menu to configure external connection for this port group.

**Participation** – Use the pull-down menu to configure a interface to participate in this port group. The factory default is ‘Exclude’. The possible values are:

- Include: This interface is the member of the port group.
- Exclude: This interface is not the member of the port group.

**Non-Configurable Data**

**Slot/Port** – The interface

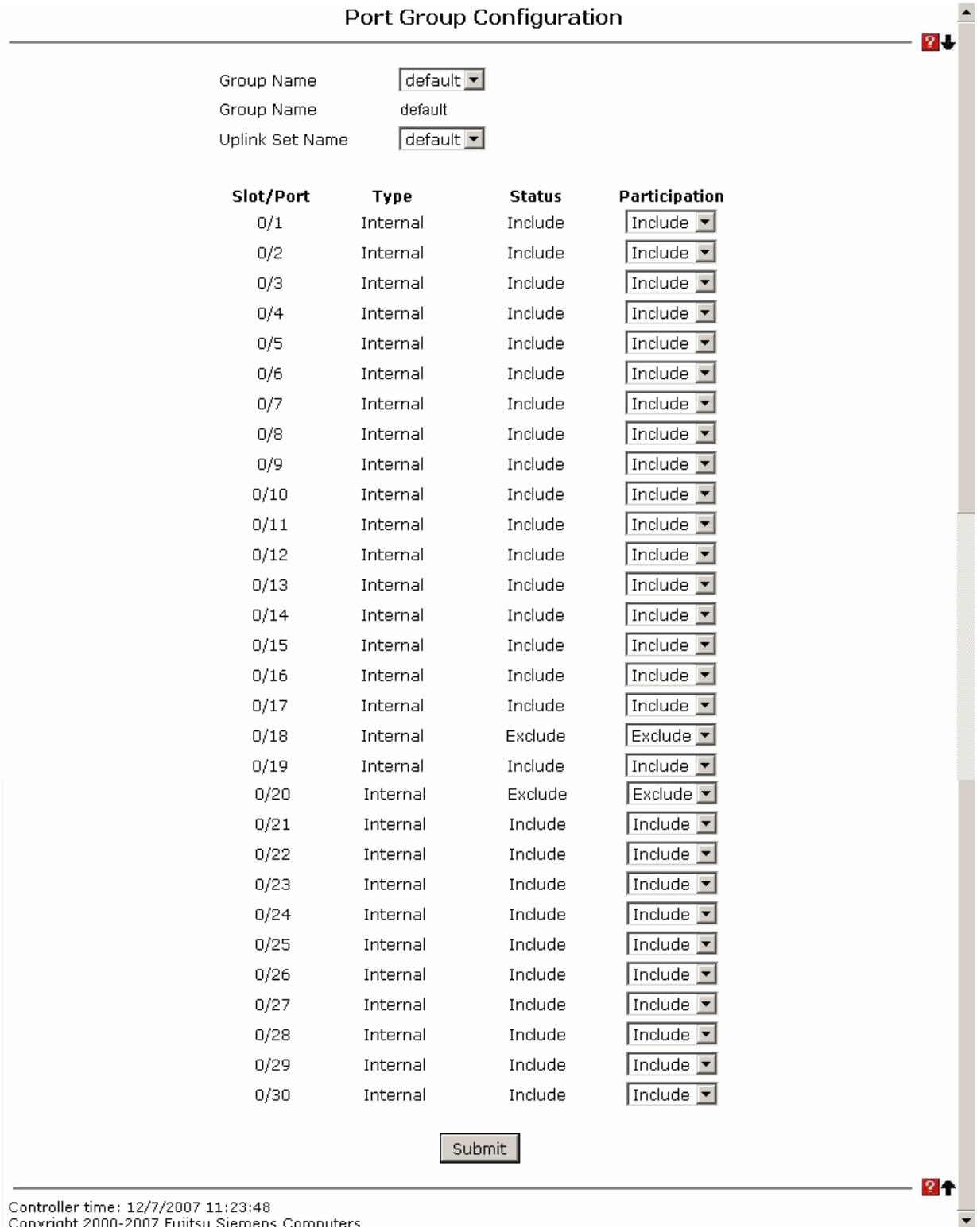
**Type** – The interface type. Type should be internal.

**Status** – The interface is belong to this port group or not.

### Command Buttons

**Submit** – Update the IBP the values on this screen. If you want the IBP to retain the new values across a power cycle, you have to perform a save.

**Delete** - Delete the port group. You are not allowed to delete the "default" port group.



#### 6.2.1.2.2. Viewing Port Group Information Page

This page displays the status of all currently configured port group.

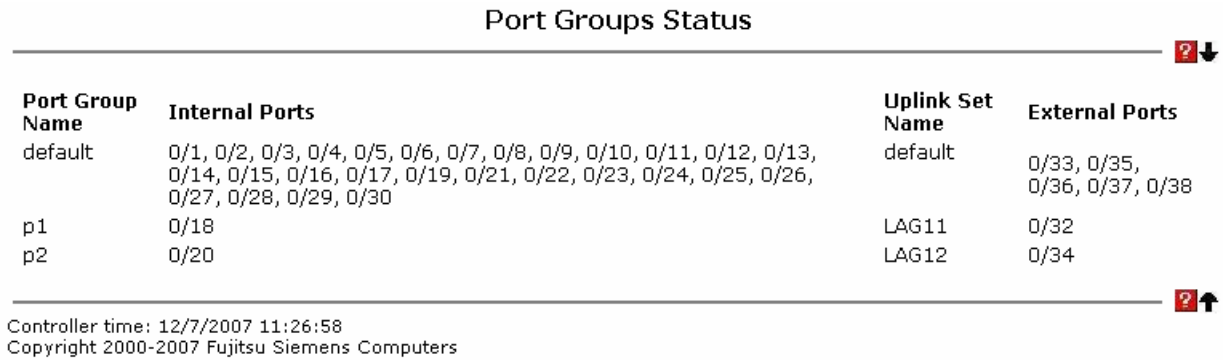
**Non-Configurable Data**

**Port Group Name** – The group name of the port group.

**Internal Ports** – List the internal port members.

**Uplink Set Name** –The name of the uplink set.

**External Ports** – List the external port members.



Port Groups Status

| Port Group Name | Internal Ports | Uplink Set Name | External Ports |
|---|---|---|---|
| default | 0/1, 0/2, 0/3, 0/4, 0/5, 0/6, 0/7, 0/8, 0/9, 0/10, 0/11, 0/12, 0/13, 0/14, 0/15, 0/16, 0/17, 0/19, 0/21, 0/22, 0/23, 0/24, 0/25, 0/26, 0/27, 0/28, 0/29, 0/30 | default | 0/33, 0/35, 0/36, 0/37, 0/38 |
| p1 | 0/18 | LAG11 | 0/32 |
| p2 | 0/20 | LAG12 | 0/34 |

Controller time: 12/7/2007 11:26:58
Copyright 2000-2007 Fujitsu Siemens Computers

### 6.2.1.3 Managing VLAN Port Groups

#### 6.2.1.3.1. Configuring VLAN Port Group Configuration Page

The purpose of the VLAN port group configuration is to create groups based on the VLAN basis, and to modify the existing groups. Only the internal ports could be defined to be the member of the VLAN port groups. The external connection is defined by specifying an Uplink Set.

**Selection Criteria**

**VLAN Port Group Name** – You can use this screen to configure an existing VLAN Port Group, or to create a new one. Use this pulldown menu to select one of the existing VLAN Port Groups, or select 'Create' to add a new one.

**Configurable Data**

**VLAN Port Group Name** – Specify the name for the new VLAN Port Group. It can be up to 32 alphanumeric characters, including blanks.

**VLAN ID** – the VLAN Identifier for the VLAN Port Group. The range of the VLAN ID is from 1 to 4094.

**Uplink Set Name** – Specify the uplink set for the external connection. If the pulldown menu shows "----------", it means that there is no available uplink set.

**Participation** – Use the pull-down menu to configure a interface to participate in this VLAN port group. The factory default is ‘Exclude’. The possible values are:

- Include: This interface is the member of the VLAN port group.
- Exclude: This interface is not the member of the VLAN port group.

**Native VLAN** – Use the pull-down menu to configure a VLAN group to behavior as the Native VLAN port group.

- Enable: Enabling this VLAN Port Group to be a Native VLAN Port Group.
- Disable: Disabling this Native VLAN Port Group.

**Non-Configurable Data**

**Slot/Port** – The interface

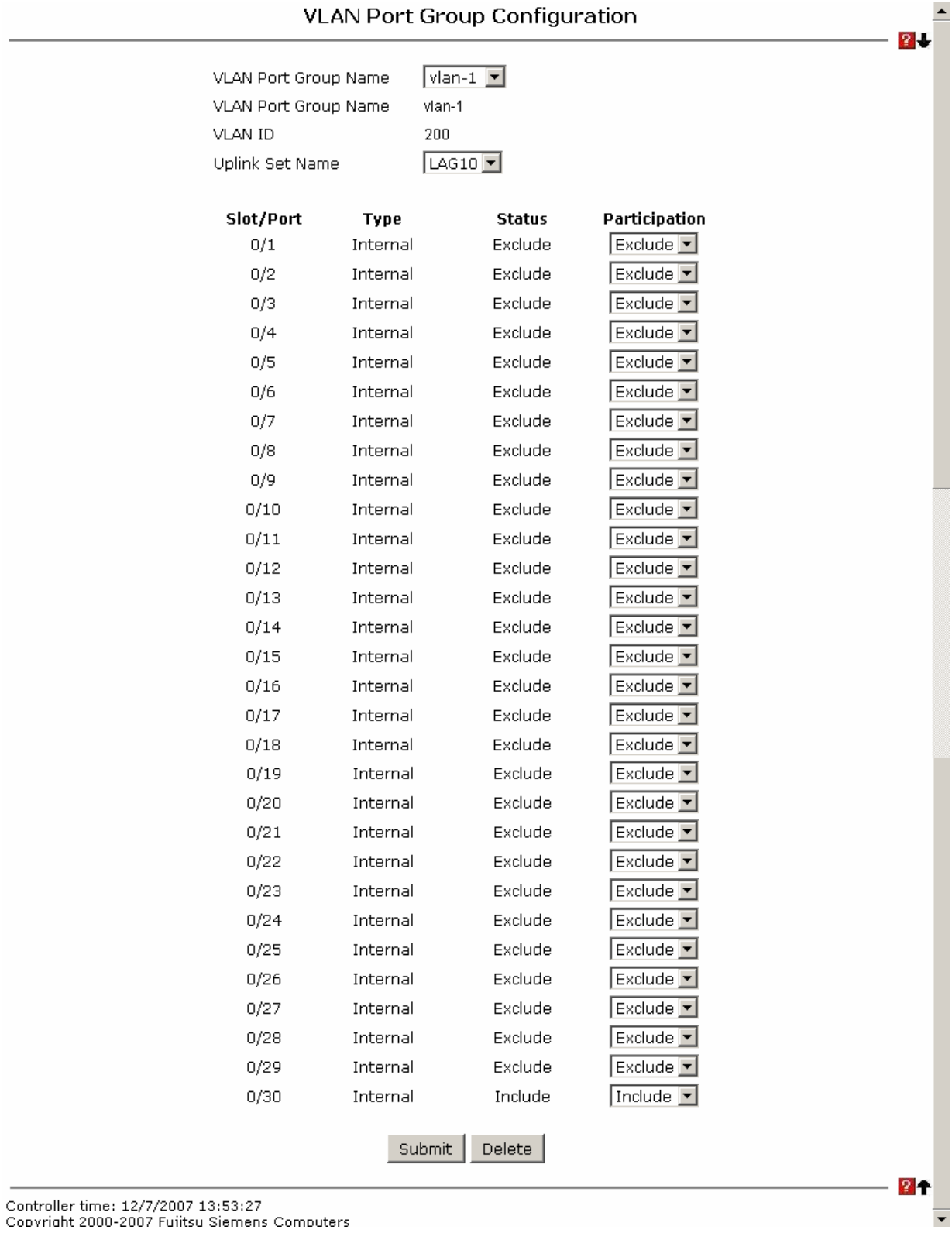
**Type** – The interface type. Type should be internal.

**Status** –Indicates the current value of the participation parameter for the interface.

**Command Buttons**

**Submit** – Update the IBP the values on this screen. If you want the IBP to retain the new values across a power cycle, you have to perform a save.

**Delete** - Delete the VLAN port group.




### 6.2.1.3.2. Viewing VLAN Port Group Information Page

This page displays the status of all currently configured VLAN port group.

**Non-Configurable Data**

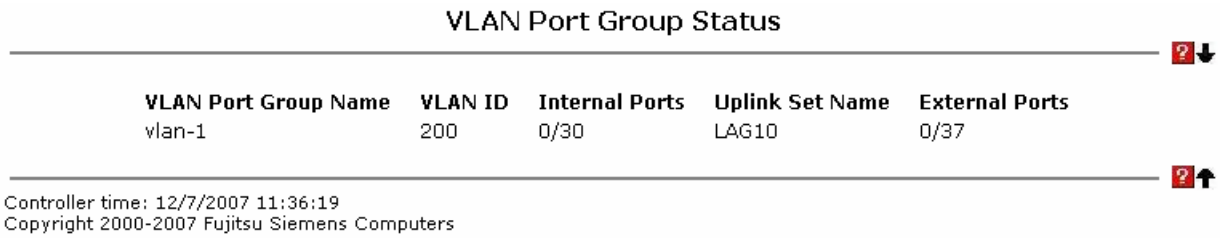
**VLAN Port Group Name** – The group name of the VLAN port group.

**VLAN ID** – The VLAN Identifier of the VLAN Port Group.

**Internal Ports** – Internal interface, member of that VLAN Port Group.

**Uplink Set Name** – The Uplink Set for the external connection of that VLAN Port Group.

**External Ports** – External interface, member of the specified Uplink Set.



### 6.2.1.4 Managing Service LAN Groups

#### 6.2.1.4.1. Configuring Service LAN Configuration Page

**Selection Criteria**

**Service LAN Name** – You can use this screen to configure an existing Service LAN, or to create a new one. Use this pulldown menu to select one of the existing Service LAN Groups, or select 'Create' to add a new one.

**Configurable Data**

**Service LAN Name** – Specify the name for the new Service LAN. It can be up to 32 alphanumeric characters, including blanks.

**Service LAN ID** – the VLAN Identifier for the Service LAN. The range of the VLAN ID is from 1 to 4094.

**Uplink Set Name** – Specify the uplink set for the external connection. If the pulldown menu shows "----------", it means that there is no available uplink set.

**Participation** – Use the pull-down menu to configure a interface to participate in this Service LAN. The factory default is ‘Exclude’. The possible values are:

- Include: This interface is the member of the Service LAN.
- Exclude: This interface is not the member of the Service LAN.

**Non-Configurable Data**

**Slot/Port** – The interface

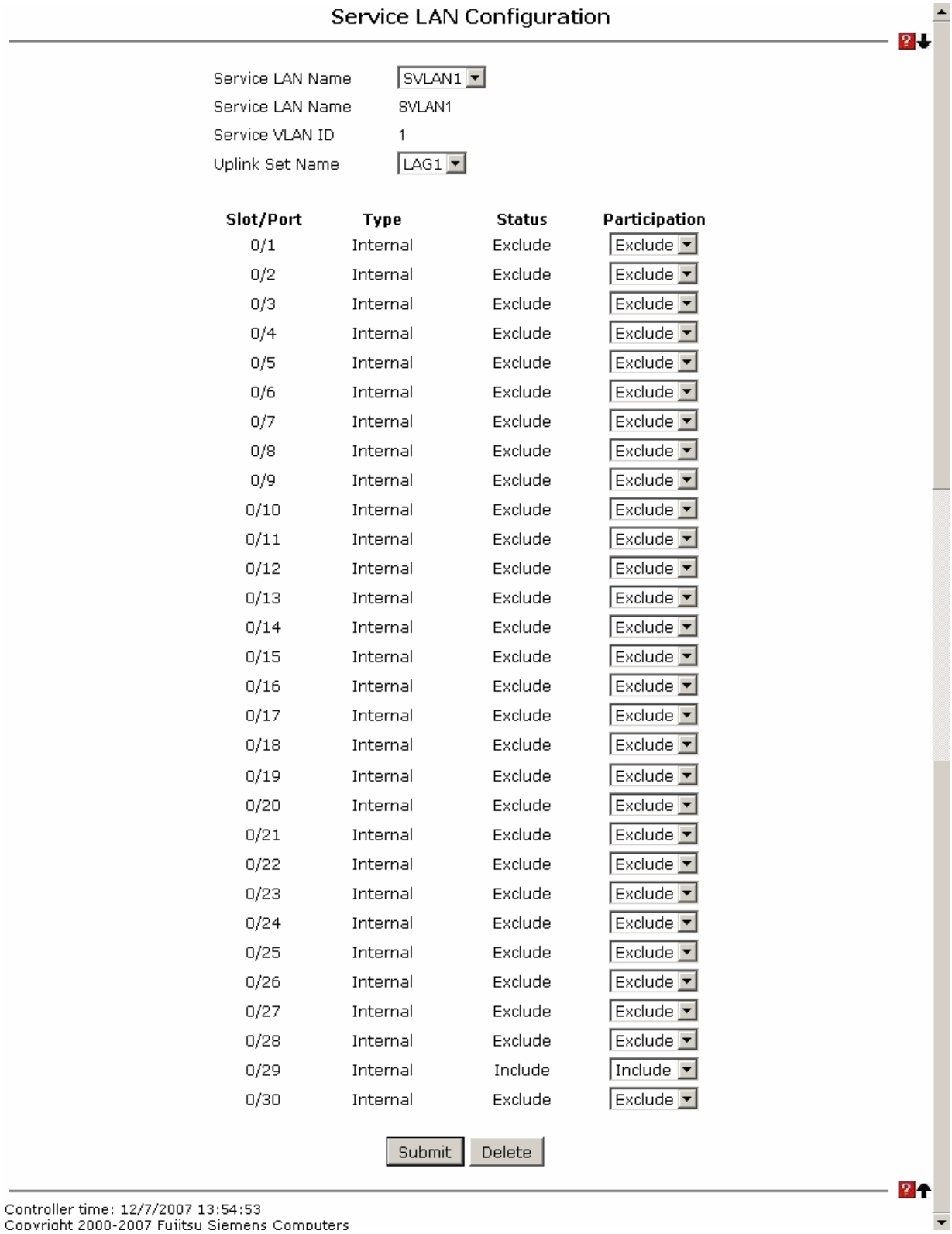
**Type** – The interface type. Type should be internal.

**Status** –Indicates the current value of the participation parameter for the interface.

**Command Buttons**

**Submit** – Update the IBP the values on this screen. If you want the IBP to retain the new values across a power cycle, you have to perform a save.

**Delete** - Delete the Service LAN.




### 6.2.1.4.2. Viewing Service LAN Information Page

This page displays the status of all currently configured Service LAN.

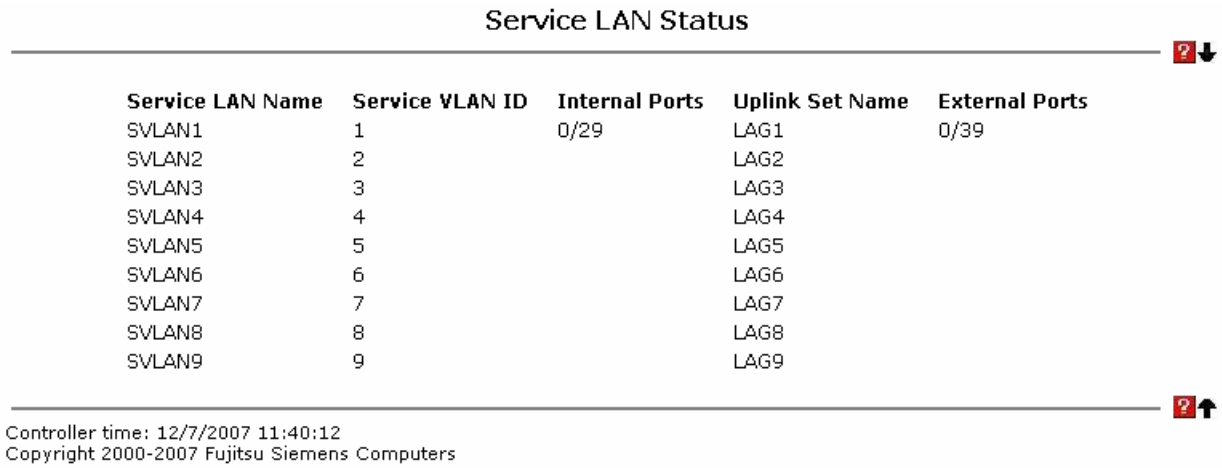
**Non-Configurable Data**

**Service LAN Name** – The group name of the Service LAN.

**Internal Ports** – Internal interface, member of that Service LAN.

**Uplink Set Name** – The Uplink Set for the external connection of that Service LAN.

**External Ports** – External interface, member of the specified Uplink Set.



Service LAN Status

| Service LAN Name | Service VLAN ID | Internal Ports | Uplink Set Name | External Ports |
|---|---|---|---|---|
| SVLAN1 | 1 | 0/29 | LAG1 | 0/39 |
| SVLAN2 | 2 | | LAG2 | |
| SVLAN3 | 3 | | LAG3 | |
| SVLAN4 | 4 | | LAG4 | |
| SVLAN5 | 5 | | LAG5 | |
| SVLAN6 | 6 | | LAG6 | |
| SVLAN7 | 7 | | LAG7 | |
| SVLAN8 | 8 | | LAG8 | |
| SVLAN9 | 9 | | LAG9 | |

Controller time: 12/7/2007 11:40:12
Copyright 2000-2007 Fujitsu Siemens Computers

### 6.2.1.5 Managing Service VLAN Groups

#### 6.2.1.5.1. Configuring Service VLAN Configuration Page

**Selection Criteria**

**Service VLAN Name** - You can use this screen to reconfigure an existing Service VLAN, or to create a new one. Use this pull down menu to select one of the existing Service VLANs, or select 'Create' to add a new one.

**Configurable Data**

**Service VLAN Name** – Specify the Service VLAN Name for the new Service VLAN. It can be up to 32 alphanumeric characters, including blanks.

**Service VLAN ID** - Specify the VLAN Identifier for the new Service VLAN. (You can only enter data in this field when you are creating a new Service VLAN.) The range of the VLAN ID is from 1 to 4094.

**Uplink Set Name** – Specify the uplink set for the external connection. If the pulldown menu shows "----------", it means that there is no available uplink set.

**Participation** – Use the pull-down menu to configure a interface to participate in this Service VLAN. The factory default is ‘Exclude’. The possible values are:

- Include: This interface is the member of the Service VLAN.
- Exclude: This interface is not the member of the Service VLAN.

**Non-Configurable Data**

**Slot/Port** - Indicates the interface.

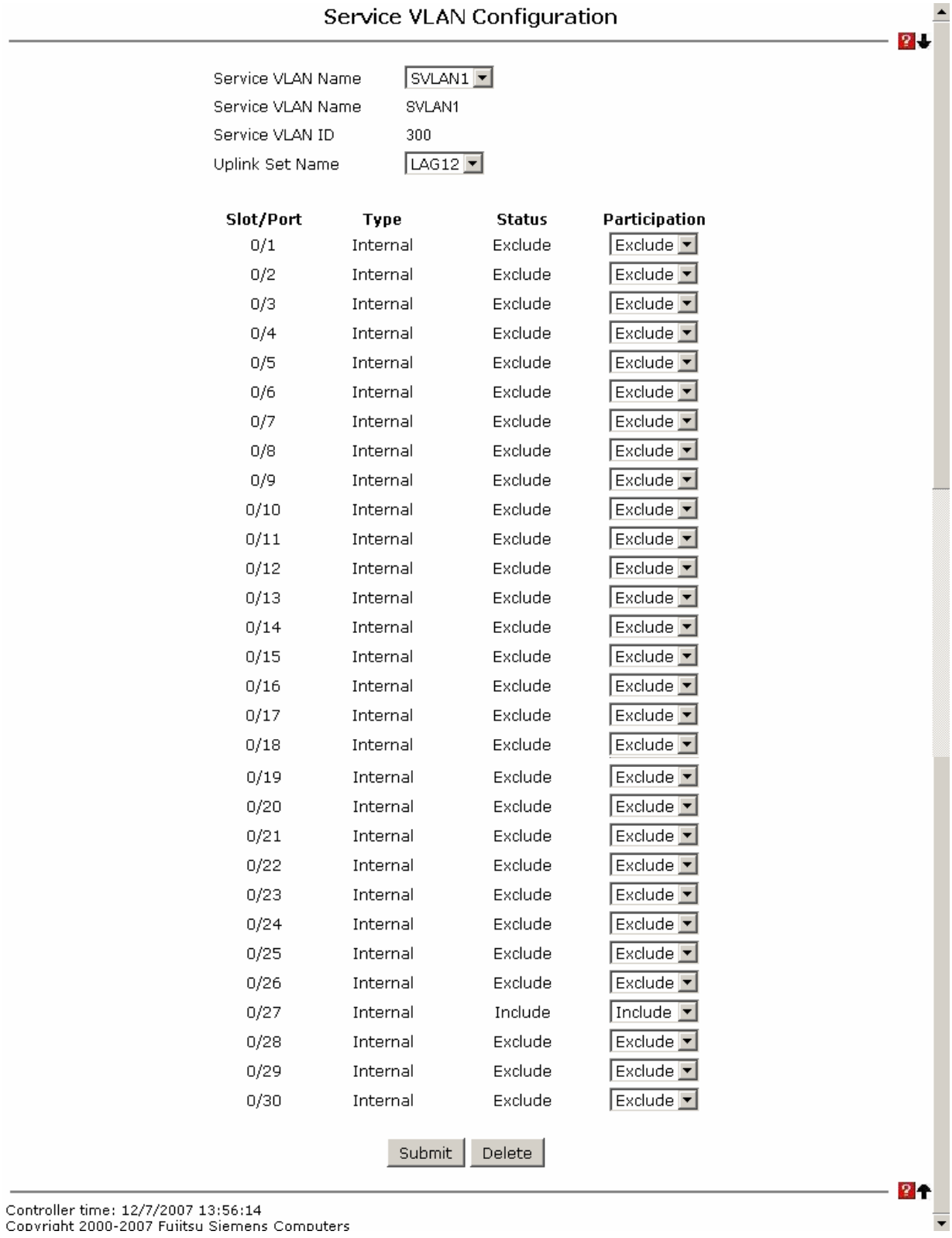
**Type** – The interface type. Type could be Internal.

**Status** - Indicates the current value of the participation parameter for the interface.

**Command Buttons**

**Submit** - Update the IBP with the values on this screen. If you want the IBP to retain the new values across a power cycle, you must perform a save.

**Delete** - Delete this Service VLAN.




### 6.2.1.5.2. Viewing Service VLAN Information Page

This page displays the status of all currently configured Service VLANs.

**Non-Configurable Data**

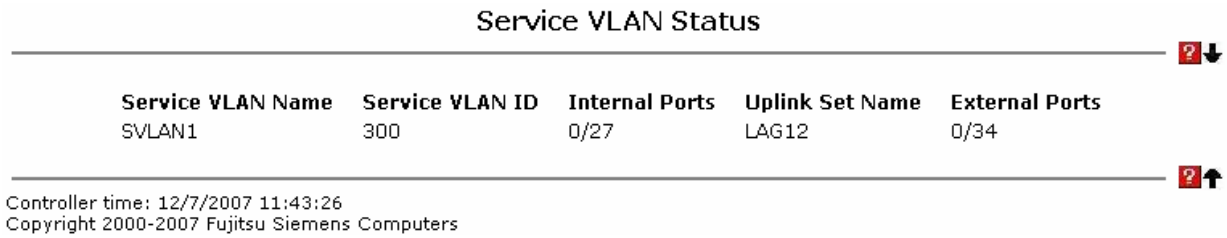
**Service VLAN Name** – The group name of the Service VLAN.

**Service VLAN ID** –The VLAN Identifier of the Service VLAN.

**Internal Ports** – Internal interface, member of that Service VLAN.

**Uplink Set Name** – The Uplink Set for the external connection of that Service VLAN.

**External Ports** – External interface, member of the specified Uplink Set.



### 6.2.1.6 Managing Port Backup

#### 6.2.1.6.1. Configuring Port Backup Configuration Page

Two link aggregation groups are associated with one uplink set as the uplink set is created. Two link aggregation groups are defined as active and backup port internally. One of two link aggregation groups will be activated at a time. For example, as active link aggregation group is link up, the backup aggregation group will be blocked (no traffic could be sent or received). Otherwise, if active aggregation group is link down (all members of the active aggregation group are link down), the backup aggregation group will be activated. As the active aggregation group is link up again, the backup one will be deactivated.

**Configurable Data**

**Active/Backup** – Select field to set the interface to be in active aggregation group or backup aggregation group.

**Non-Configurable Data**

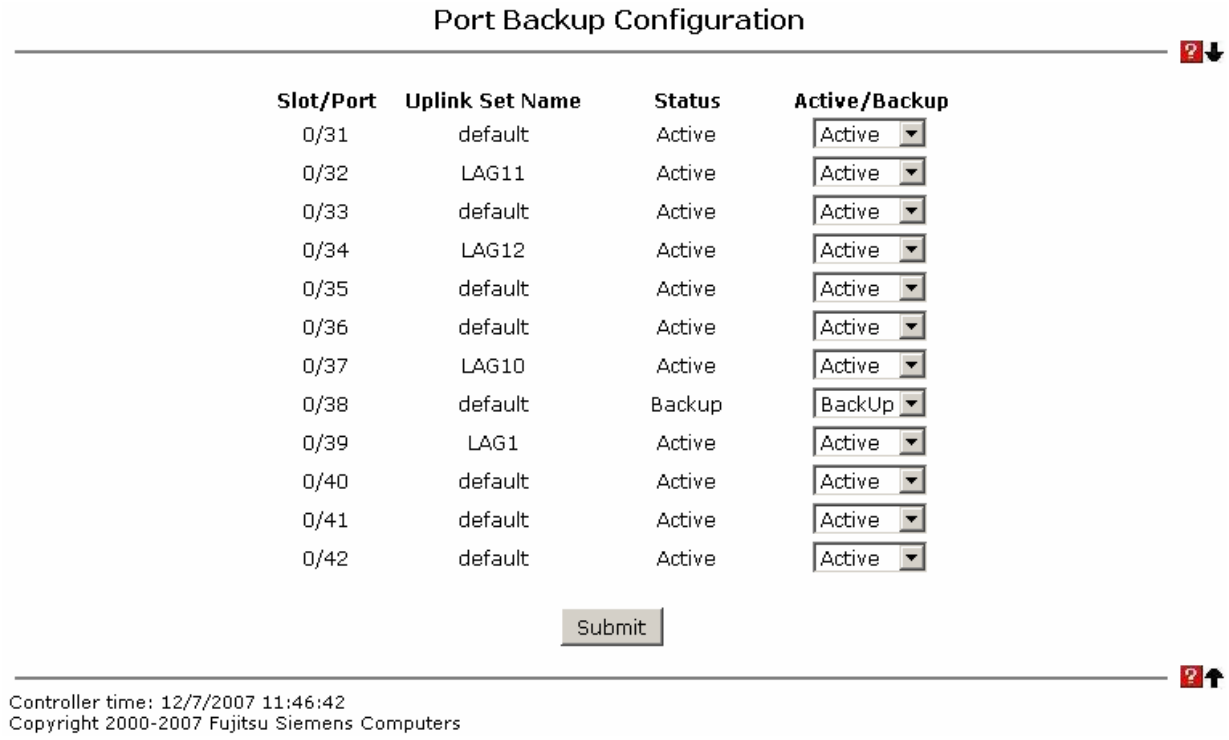
**Slot/Port** – The interface.

**Port Group** – The name of port group that this interface belongs to.

**Status** – Active or Backup.

**Command Buttons**

**Submit** – Update the IBP with the values on this screen. If you want the IBP to retain the new values across a power cycle, you have to perform a save.




### 6.2.1.6.2. Viewing Port Backup Status Page

The page displays the status of all currently configured port-backup.

**Non-Configurable Data**

**Uplink Set Name** – The name of the Uplink Set.

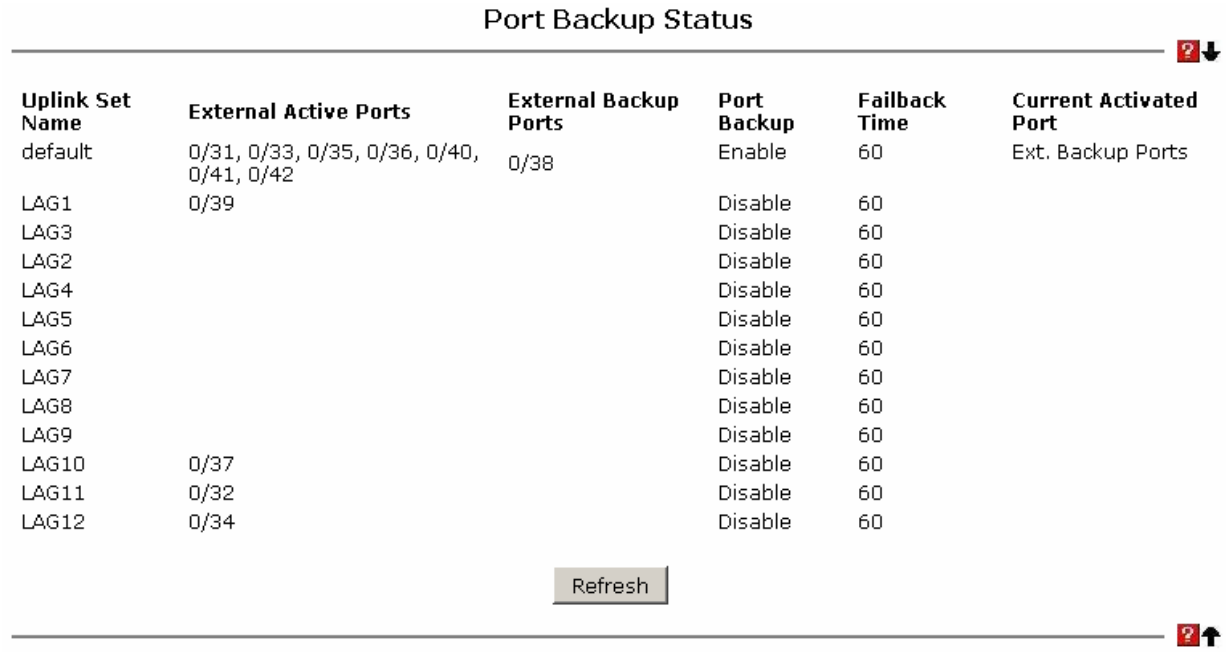
**External Active Ports** – The configured external active ports.

**External Backup Ports** – The configured external backup ports.

**Port Backup** – Current port backup setting for the Uplink Set.

**Failback Time** –The time delay for activating the active port if the link of active port is resumed.

**Current Activated Port** – Current activated port for the Uplink Set.



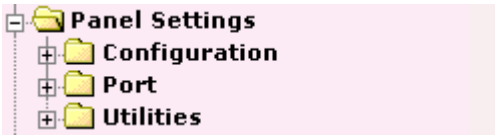
Port Backup Status

| Uplink Set Name | External Active Ports | External Backup Ports | Port Backup | Failback Time | Current Activated Port |
|---|---|---|---|---|---|
| default | 0/31, 0/33, 0/35, 0/36, 0/40, 0/41, 0/42 | 0/38 | Enable | 60 | Ext. Backup Ports |
| LAG1 | 0/39 | | Disable | 60 | |
| LAG3 | | | Disable | 60 | |
| LAG2 | | | Disable | 60 | |
| LAG4 | | | Disable | 60 | |
| LAG5 | | | Disable | 60 | |
| LAG6 | | | Disable | 60 | |
| LAG7 | | | Disable | 60 | |
| LAG8 | | | Disable | 60 | |
| LAG9 | | | Disable | 60 | |
| LAG10 | 0/37 | | Disable | 60 | |
| LAG11 | 0/32 | | Disable | 60 | |
| LAG12 | 0/34 | | Disable | 60 | |

Refresh

Controller time: 12/7/2007 11:48:28
Copyright 2000-2007 Fujitsu Siemens Computers

### 6.2.2 Panel Settings Menu




#### 6.2.2.1 Configuring Management Session and Network Parameters

##### 6.2.2.1.1 Viewing Inventory Information

Use this panel to display the IBP's Vital Product Data, stored in non-volatile memory at the factory.

**Non-Configurable Data**

**System Description** - The product name of this IBP module.

**Machine Type** - The machine type of this IBP module.

**Machine Model** - The model within the machine type.

**Serial Number** - The unique box serial number for this IBP module.

**Part Number** - The manufacturing part number.

**Base MAC Address** - The burned-in universally administered MAC address of this IBP module.

**Hardware Version** - The hardware version of this IBP module. It is divided into four parts. The first byte is the major version and the second byte represents the minor version.

**Loader Version** - The release-version maintenance number of the loader code currently running on the IBP module. For example, if the major version was 2, and the minor version was 4, the format would be '2.4'.

**Boot Rom Version** - The release-version maintenance number of the boot rom code currently running on the IBP module. For example, if the major version was 2, and the minor version was 4, the format would be '2.4'.

**Label Revision Number** - The label revision serial number of this IBP module is used for manufacturing purpose.

**Runtime Version** - The release-version maintenance number of the code currently running on the IBP module. For example, if the major version was 2, and the minor version was 4, the format would be '2.4'.

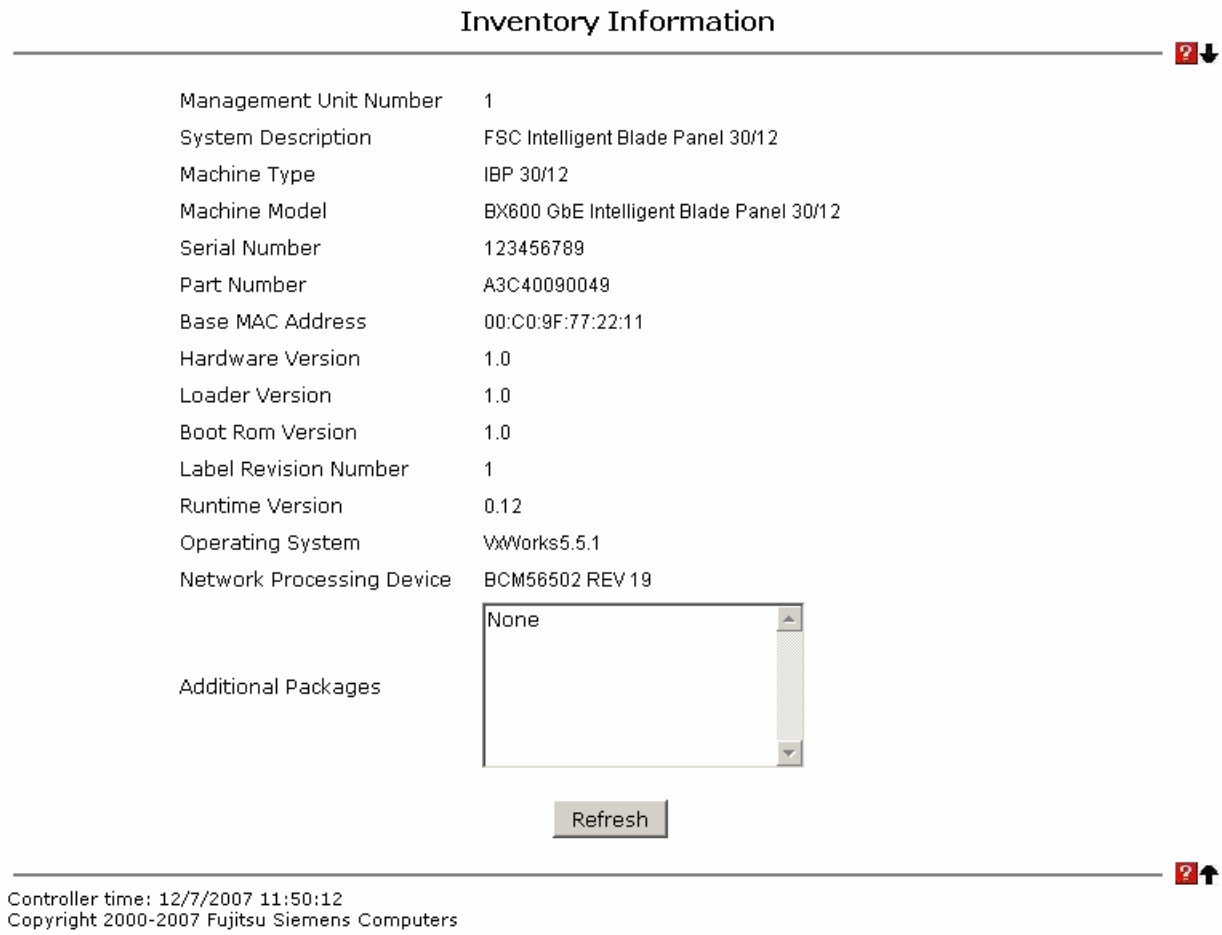
**Operating System** - The operating system currently running on the IBP module.

**Network Processing Device** - Identifies the network processor hardware.

**Additional Packages** - A list of the optional software packages installed on the IBP module, if any.

**Command Buttons**

**Refresh** - Updates the information on the page.


Inventory Information
Management Unit Number 1
System Description FSC Intelligent Blade Panel 30/12
Machine Type IBP 30/12
Machine Model BX600 GbE Intelligent Blade Panel 30/12
Serial Number 123456789
Part Number A3C40090049
Base MAC Address 00:C0:9F:77:22:11
Hardware Version 1.0
Loader Version 1.0
Boot Rom Version 1.0
Label Revision Number 1
Runtime Version 0.12
Operating System VxWorks5.5.1
Network Processing Device BCM56502 REV 19
Additional Packages
None
Refresh
Controller time: 12/7/2007 11:50:12
Copyright 2000-2007 Fujitsu Siemens Computers

#### 6.2.2.1.2 Viewing Panel Description Page

**Configurable Data**

**System Name** - Enter the name you want to use to identify this IBP module. You may use up to 31 alpha-numeric characters. The factory default is blank.

**System Location** - Enter the location of this IBP module. You may use up to 31 alpha-numeric characters. The factory default is blank.

**System Contact** - Enter the contact person for this IBP module. You may use up to 31 alpha-numeric characters. The factory default is blank.

**Non-Configurable Data**

**System Description** - The product name of this IBP module.

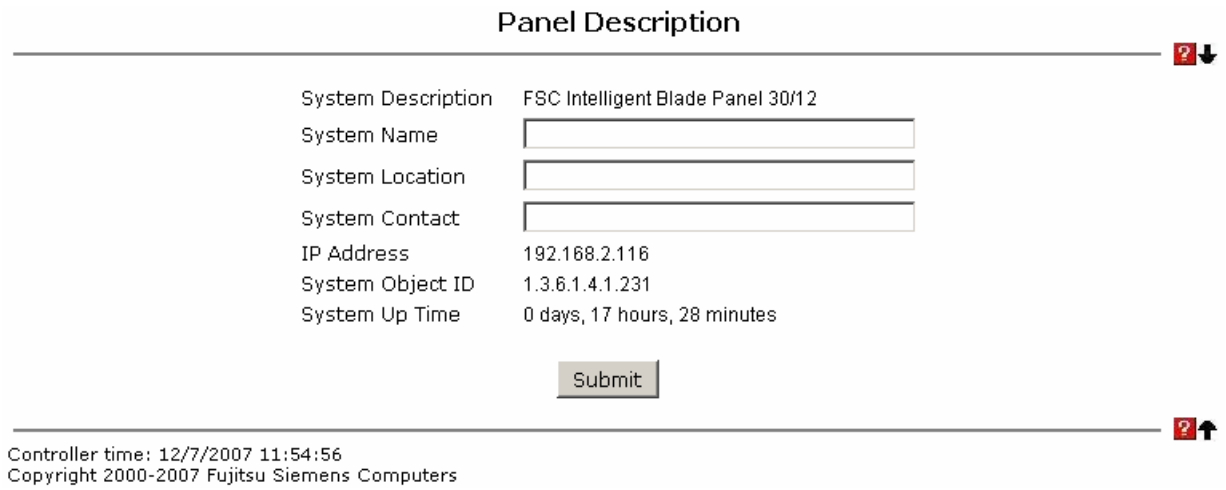
**System Object ID** - The base object ID for the IBP's enterprise MIB.

**System IP Address** - The IP Address assigned to the network interface.

**System Up time** - The time in days, hours and minutes since the last IBP module reboot.

**Command Buttons**

**Submit** - Update the IBP module with the values on the screen. If you want the IBP module to retain the new values across a power cycle you must perform a save.



#### 6.2.2.1.3 Configuring Inband Administration Page

The network interface is the logical interface used for in-band connectivity with the IBP module via any of the IBP's front panel ports. The configuration parameters associated with the IBP's network interface do not affect the configuration of the front panel ports through which traffic is switched or routed.

To access the IBP module over a network you must first configure it with IP information (IP address, subnet mask, and default gateway). You can configure the IP information using any of the following:

**BOOTP**

**DHCP**

**Terminal interface via the EIA-232 port**

Once you have established in-band connectivity, you can change the IP information using any of the following:

**Terminal interface via the EIA-232 port**

**Terminal interface via telnet**

**SNMP-based management**

**Web-based management**

**Configurable Data**

**IP Address** - The IP address of the interface. The factory default value is 0.0.0.0

**Subnet Mask** - The IP subnet mask for the interface. The factory default value is 0.0.0.0

**Default Gateway** - The default gateway for the IP interface. The factory default value is 0.0.0.0

**Network Configuration Protocol Current** - Choose what the IBP module should do following power-up: transmit a Bootp request, transmit a DHCP request, or do nothing (none). The factory default is None.

You cannot make this choice for both the network configuration protocol and the service port. You will only be given the choices for Bootp or DHCP here if the service port protocol is configured to None.

**Inband Administration VLAN ID** - Specifies the inband administration VLAN ID of the IBP module. It may be configured to any value in the range of 1 - 4094. The inband administration VLAN is used for management of the IBP module. This field is configurable for administrative users and read-only for other users.

**Web Mode** - Specify whether the IBP may be accessed from a Web browser. If you choose to enable web mode you will be able to manage the IBP from a Web browser. The factory default is enabled.

**Java Mode** - Enable or disable the java applet that displays a picture of the IBP module at the top right of the screen. If you run the applet you will be able to click on the picture of the IBP to select configuration screens instead of using the navigation tree at the left side of the screen. The factory default is enabled.

**Web Port** - This field is used to set the HTTP Port Number. The value must be in the range of 1 to 65535. Port 80 is the default value. The currently configured value is shown when the web page is displayed.

**Paticipation** – This select field is used to set the interface to be grated or denied for

management access. By setting the interface to be granted, IBP will be allowed to access from this interface; on the other hand, if the interface is set to be denied, IBP will not be allowed to access from this interface.

### Non-Configurable Data

**Burned-in MAC Address** - The burned-in MAC address used for in-band connectivity if you choose not to configure a locally administered address.

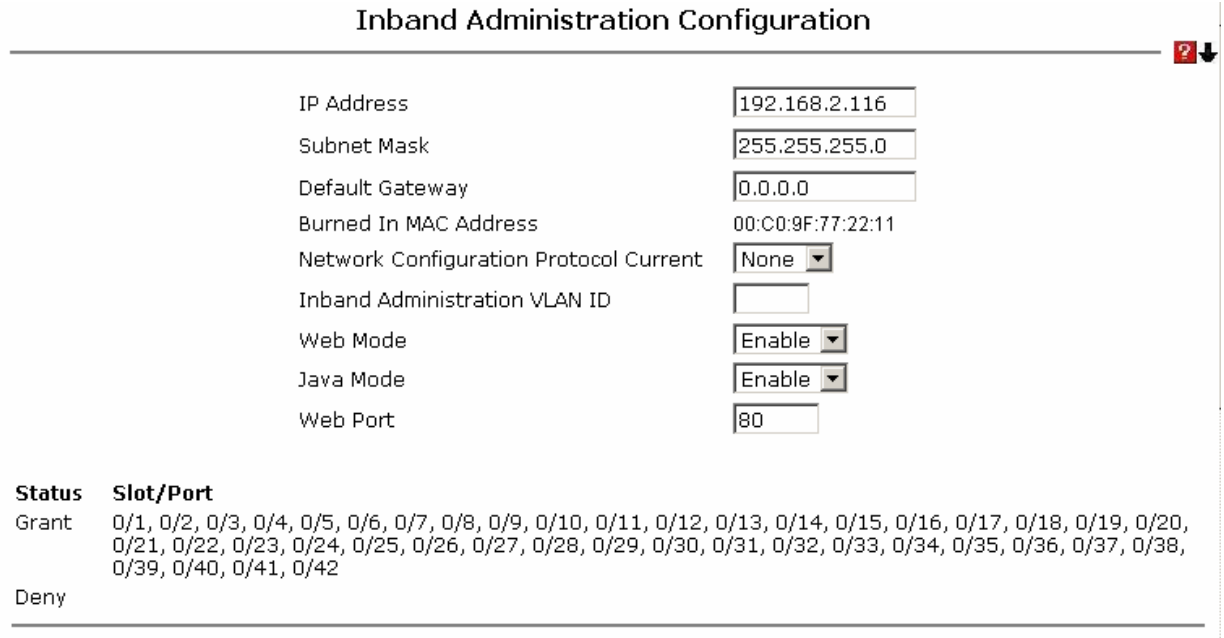
**Status** – The status of the interface. Grant or Deny.

**Slot/Port** – The interface

**Type** – The interface type. Type could be Internal or External.

### Command Buttons

**Submit** - Update the IBP module with the values on the screen. If you want the IBP module to retain the new values across a power cycle you must perform a save.



#### 6.2.2.1.4 Configuring Telnet Session Page

**Configurable Data**

**Telnet Session Timeout (minutes)** - Specify how many minutes of inactivity should occur on a telnet session before the session is logged off. You may enter any number from 1 to 160. The factory default is 5.

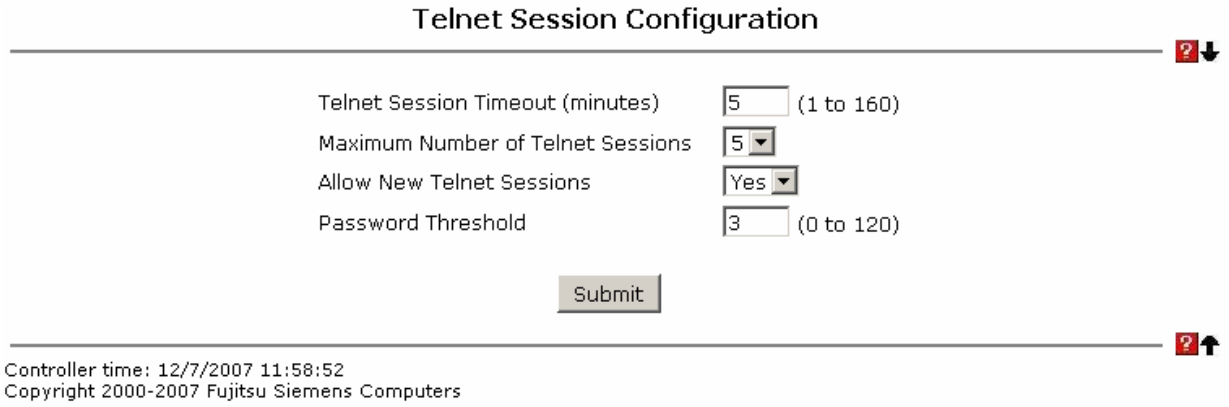
**Maximum Number of Telnet Sessions** - Use the pulldown menu to select how many simultaneous telnet sessions will be allowed. The maximum is 5, which is also the factory default.

**Allow New Telnet Sessions** - If you set this to no, new telnet sessions will not be allowed. The factory default is yes.

**Password Threshold** - When the logon attempt threshold is reached on the console port, the system interface becomes silent for a specified amount of time before allowing the next logon attempt. (Use the silent time command to set this interval.) When this threshold is reached for Telnet, the Telnet logon interface closes. The default value is 3.

**Command Buttons**

**Submit** - Update the IBP module with the values on the screen. If you want the IBP module to retain the new values across a power cycle you must perform a save



#### 6.2.2.1.5 Configuring Outbound Telnet Client Configuration Page

**Configurable Data**

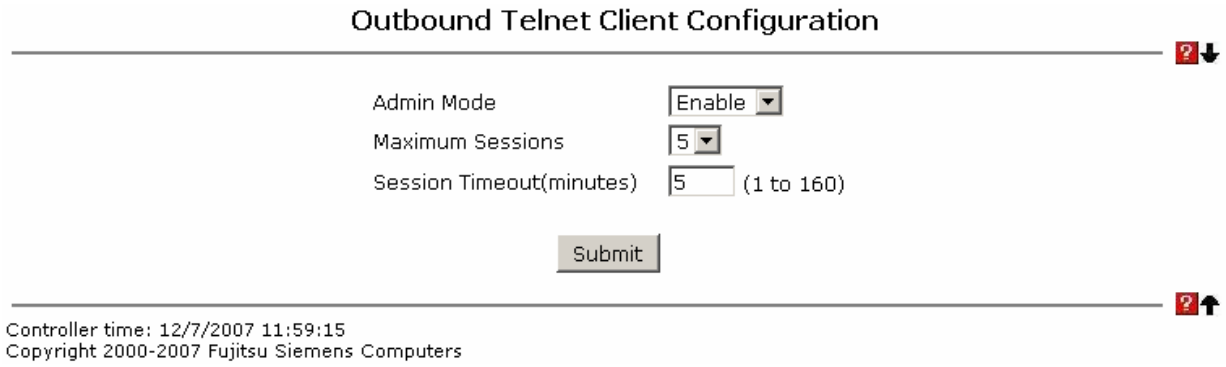
**Admin Mode** - Specifies if the Outbound Telnet service is Enabled or Disabled. Default value is Enabled.

**Maximum Sessions** - Specifies the maximum number of Outbound Telnet Sessions allowed. Default value is 5. Valid Range is (0 to 5).

**Session Timeout** - Specifies the Outbound Telnet login inactivity timeout. Default value is 5. Valid Range is (1 to 160).

**Command Buttons**

**Submit** - Sends the updated configuration to the IBP module. Configuration changes take effect immediately.



#### 6.2.2.1.6 Configuring Serial Port Page

**Configurable Data**

**Serial Port Login Timeout (minutes)** - Specify how many minutes of inactivity should occur on a serial port connection before the IBP closes the connection. Enter a number between 0 and 160: the factory default is 5. ***Entering 0 disables the timeout.***

**Baud Rate (bps)** - Select the default baud rate for the serial port connection from the pull-down menu. You may choose from 1200, 2400, 4800, 9600, 19200, 38400, 57600, and 115200 baud. The factory default is 9600 baud.

**Password Threshold** - When the logon attempt threshold is reached on the console port, the system interface becomes silent for a specified amount of time before allowing the next logon attempt. (Use the silent time command to set this interval.) When this threshold is reached for Telnet, the Telnet logon interface closes. The default value is 3.

**Silent Time (Sec)** - Use this command to set the amount of time the management console is inaccessible after the number of unsuccessful logon attempts exceeds the threshold set by the password threshold command. The default value is 0.

**Non-Configurable Data**

**Character Size (bits)** - The number of bits in a character. This is always 8.

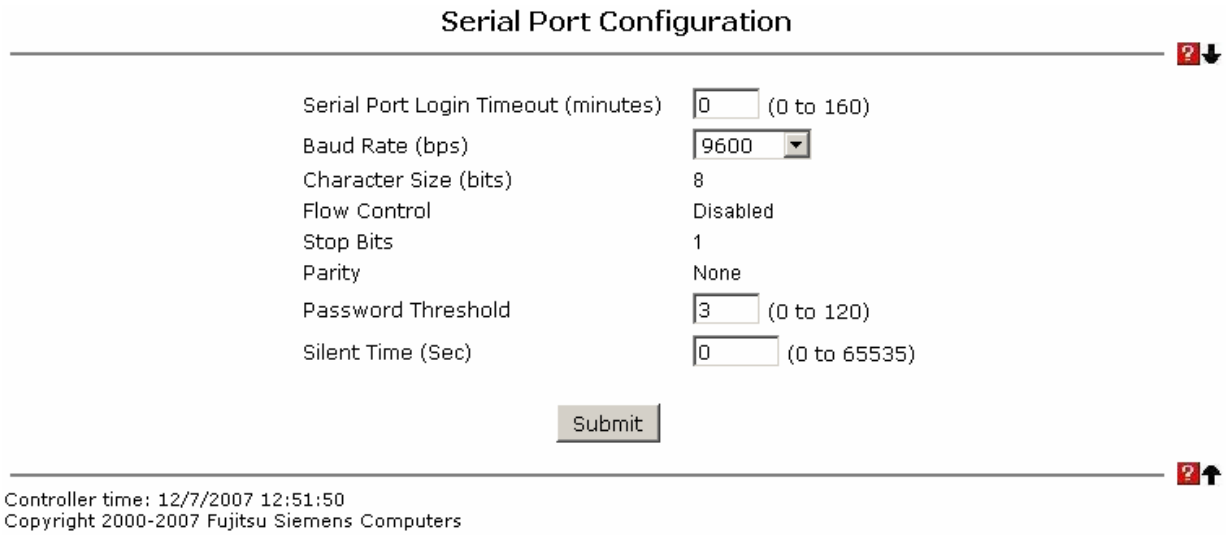
**Flow Control** - Whether hardware flow control is enabled or disabled. It is always disabled.

**Parity** - The parity method used on the serial port. It is always None.

**Stop Bits** - The number of stop bits per character. It is always 1.

**Command Buttons**

**Submit** - Update the IBP module with the values on the screen. If you want the IBP module to retain the new values across a power cycle you must perform a save.



#### 6.2.2.1.7 Defining User Accounts Page

By default, two user accounts exist:

admin, with 'Read/Write' privileges

guest, with 'Read Only' privileges

By default, the password for admin is “admin”, and password for guest is blank. The names are case insensitive.

If you logon with a user account with 'Read/Write' privileges (that is, as admin) you can use the User Accounts screen to assign passwords and set security parameters for the default accounts, and to add and delete accounts (other than admin) up to the maximum of six. Only a user with 'Read/Write' privileges may alter data on this screen, and only one account may be created with 'Read/Write' privileges.

**Selection Criteria**

**User Name Selector** - You can use this screen to reconfigure an existing account, or to create a new one. Use this pulldown menu to select one of the existing accounts, or select 'Create' to add a new one, provided the maximum of five 'Read Only' accounts has not been reached.

**Configurable Data**

**User Name** - Enter the name you want to give to the new account. (You can only enter data in this field when you are creating a new account.) User names are up to eight characters in length and are not case sensitive. Valid characters include all the alphanumeric characters as well as the dash ('-') and underscore ('_') characters.

**Password** - Enter the optional new or changed password for the account. It will not display as it is typed, only asterisks (*) will show. Passwords are up to eight alpha numeric characters in length, and are case sensitive.

**Confirm Password** - Enter the password again, to confirm that you entered it correctly. This field will not display, but will show asterisks (*).

**Authentication Protocol** - Specify the SNMPv3 Authentication Protocol setting for the selected user account. The valid Authentication Protocols are None, MD5 or SHA. If you select None, the user will be unable to access the SNMP data from an SNMP browser. If you select MD5 or SHA, the user login password will be used as the SNMPv3 authentication password, and you must therefore specify a password, and it must be eight characters.

**Encryption Protocol** - Specify the SNMPv3 Encryption Protocol setting for the selected user account. The valid Encryption Protocols are None or DES. If you select the DES Protocol you must enter a key in the Encryption Key field. If None is specified for the Protocol, the Encryption Key is ignored.

**Encryption Key** - If you selected DES in the Encryption Protocol field enter the SNMPv3 Encryption Key here. Otherwise this field is ignored. Valid keys are 8 to 64 characters. The Apply checkbox must be checked in order to change the Encryption Protocol and Encryption Key.

**Non-Configurable Data**

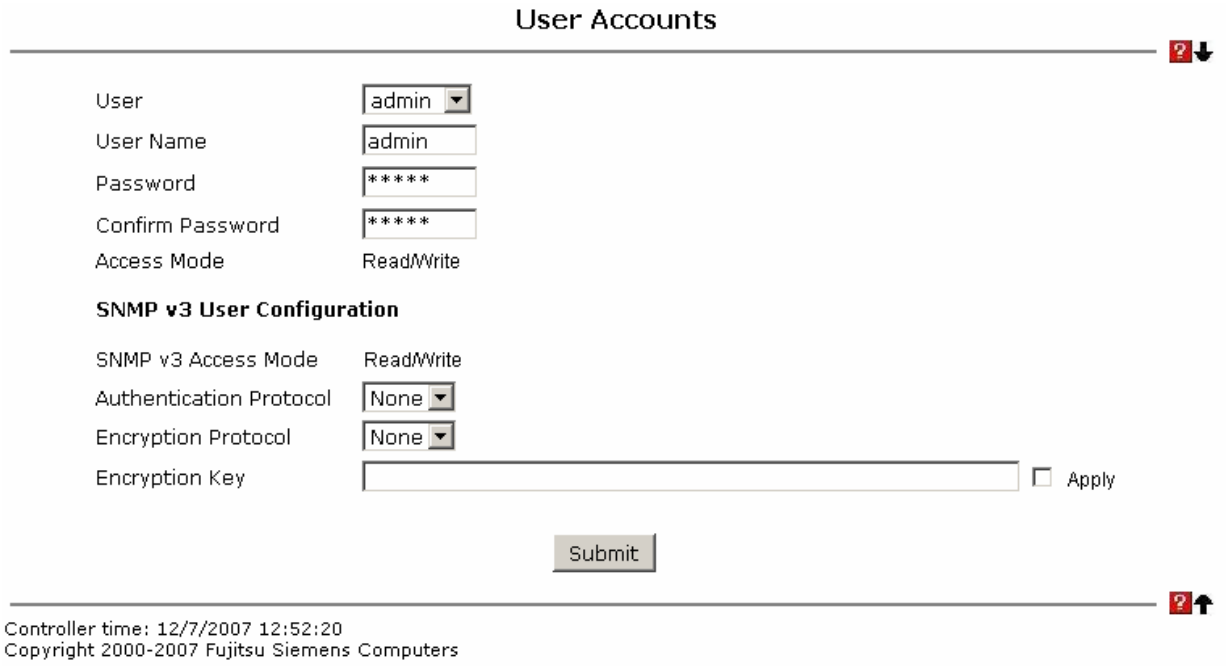
**Access Mode** - Indicates the user's access mode. The admin account always has 'Read/Write' access, and all other accounts have 'Read Only' access.

**SNMP v3 Access Mode** - Indicates the SNMPv3 access privileges for the user account. The admin account always has 'Read/Write' access, and all other accounts have 'Read Only' access.

### Command Buttons

**Submit** - Update the IBP module with the values on this screen. If you want the IBP module to retain the new values across a power cycle, you must perform a save.

**Delete** - Delete the currently selected user account. If you want the IBP module to retain the new values across a power cycle, you must perform a save. This button is only visible when you have selected a user account with 'Read Only' access. You cannot delete the 'Read/Write' user.



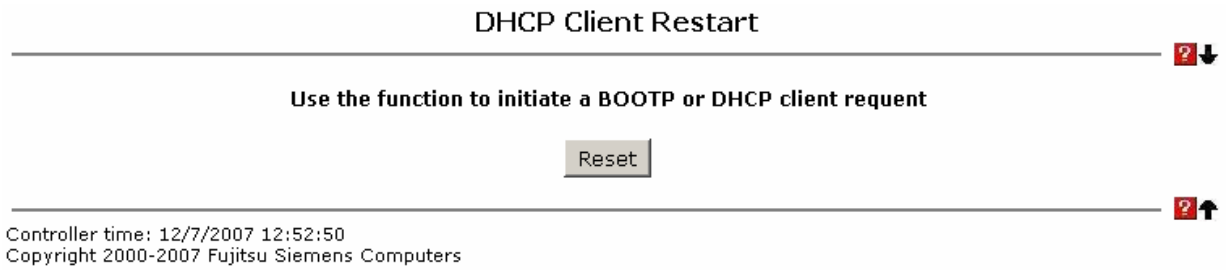
#### 6.2.2.1.8 Defining DHCP Client

**Configuring DHCP Restart Page**

This command issues a BOOTP or DHCP client request for any IP interface that has been set to BOOTP or DHCP mode via the IP address command. DHCP requires the server to reassign the client's last address if available. If the BOOTP or DHCP server has been moved to a different domain, the network portion of the address provided to the client will be based on this new domain.

**Command Buttons**

**Reset** - Send the updated screen to the IBP to restart the DHCP client.


DHCP Client Restart
Use the function to initiate a BOOTP or DHCP client request
Reset
Controller time: 12/7/2007 12:52:50
Copyright 2000-2007 Fujitsu Siemens Computers

**Configuring DHCP Client-identifier Page**

Specify the DCHP client identifier for the IBP. The DCHP client identifier is used to include a client identifier in all communications with the DHCP server. The identifier type depends on the requirements of your DHCP server.

**Non-Configurable Data**

**Current DHCP Identifier (Hex/Text)** - Shows the current setting of DHCP identifier.

**Configurable Data**

**DHCP Identifier** - Specifies the type of DHCP Identifier.

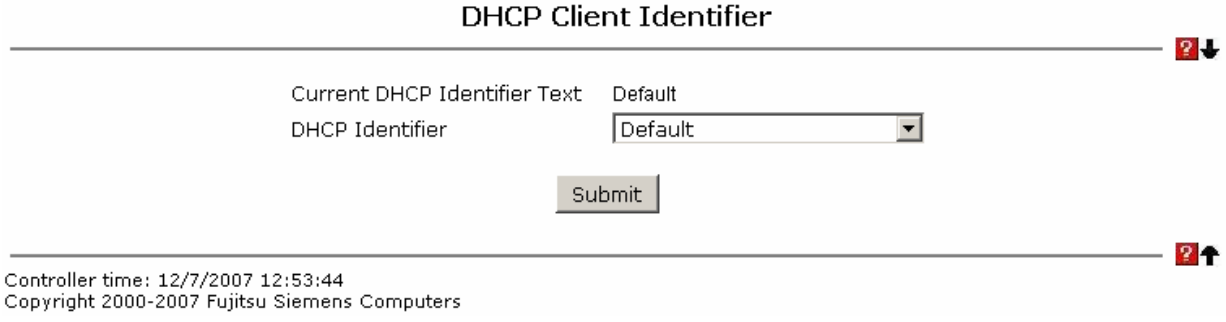
- ***Default***
- ***Specific Text String***
- ***Secific Hexadecimal Value***

**Text String** - A text string.

**Hex Value** - The hexadecimal value.

**Command Buttons**

**Submit** - Send the updated screen to the IBP perform the setting DHCP client identifier.



#### 6.2.2.1.9 Defining SNMP

**Configuring SNMP Community Configuration Page**

By default, two SNMP Communities exist:

private, with 'Read/Write' privileges and status set to enable

public, with 'Read Only' privileges and status set to enable

These are well-known communities, you can use this menu to change the defaults or to add other communities. Only the communities that you define using this menu will have access to the IBP using the SNMPv1 and SNMPv2c protocols. Only those communities with read-write level access will have access to this menu via SNMP.

You should use this menu when you are using the SNMPv1 and SNMPv2c protocol: if you want to use SNMP v3 you should use the User Accounts menu.

**Configurable Data**

**SNMP Community Name** - You can use this screen to reconfigure an existing community, or to create a new one. Use this pulldown menu to select one of the existing community names, or select 'Create' to add a new one. A valid entry is a case-sensitive string of up to 16 characters. The default community names are *public* and *private*.

**Client IP Address** - Taken together, the Client IP Address and Client IP Mask denote a range of IP addresses from which SNMP clients may use that community to access this device. If either (IP Address or IP Mask) value is 0.0.0.0, access is allowed from any IP address. Otherwise, every client's IP address is ANDed with the mask, as is the Client IP Address, and, if the values are equal, access is allowed. For example, if the Client IP Address and Client IP Mask parameters are 192.168.1.0/255.255.255.0, then any client whose IP address is 192.168.1.0 through 192.168.1.255 (inclusive) will be allowed access. To allow access from only one station, use a Client IP Mask value of 255.255.255.255, and use that machine's IP address for Client IP Address.

**Client IP Mask** - Taken together, the Client IP Address and Client IP Mask denote a range of IP addresses from which SNMP clients may use that community to access this device. If either (IP Address or IP Mask) value is 0.0.0.0, access is allowed from any IP address. Otherwise, every client's IP address is ANDed with the mask, as is the Client IP Address, and, if the values are equal, access is allowed. For example, if the Client IP Address and Client IP Mask parameters are 192.168.1.0/255.255.255.0, then any client whose IP address is 192.168.1.0 through 192.168.1.255 (inclusive) will be allowed access. To allow access from only one station, use a Client IP Mask value of 255.255.255.255, and use that machine's IP address for Client IP Address.

**Access Mode** - Specify the access level for this community by selecting Read/Write or Read Only from the pull down menu.

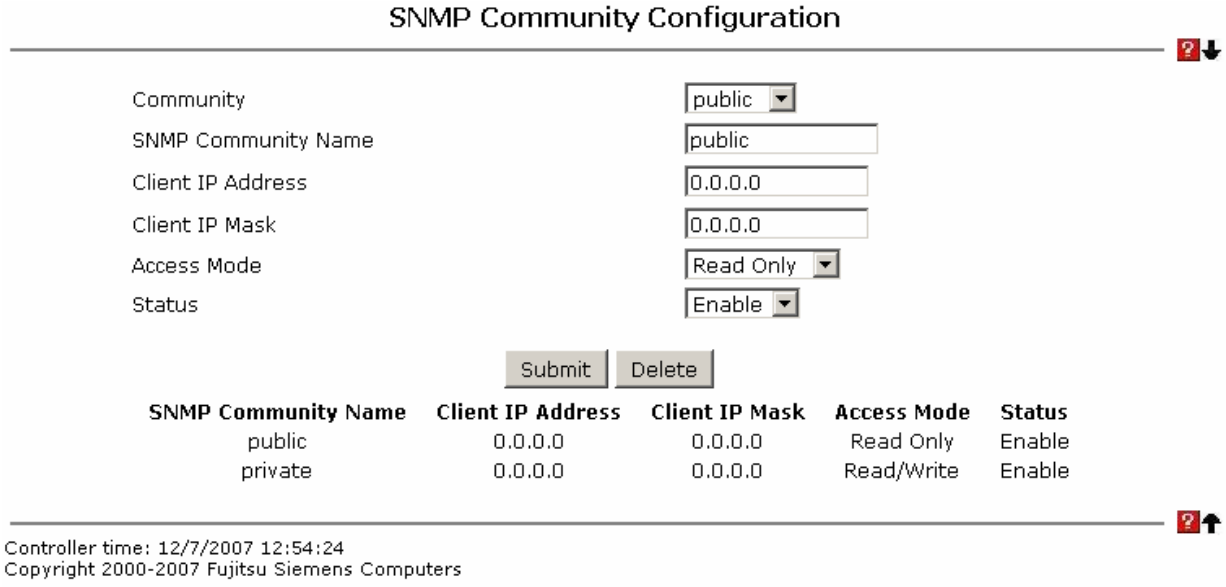
**Status** - Specify the status of this community by selecting Enable or Disable from the pull down menu. If you select enable, the Community Name must be unique among all valid Community Names or the set request will be rejected. If you select disable, the Community Name will become invalid.

**Command Buttons**

**Submit** - Update the IBP with the values on this screen. If you want the IBP to retain the new values across a power cycle, you must perform a save.

**Delete** - Delete the currently selected Community Name. If you want the IBP to retain the

new values across a power cycle, you must perform a save.




### Configuring SNMP Trap Receiver Configuration Page

This menu will display an entry for every active Trap Receiver.

### Configurable Data

**SNMP Community Name** - Enter the community string for the SNMP trap packet to be sent to the trap manager. This may be up to 16 characters and is case sensitive.

**SNMP Version** - Select the trap version to be used by the receiver from the pull down menu:

SNMP v1 - Uses SNMP v1 to send traps to the receiver.

SNMP v2 - Uses SNMP v2 to send traps to the receiver.

**IP Address** - Enter the IP address to receive SNMP traps from this device. Enter 4 numbers between 0 and 255 separated by periods.

**Status** - Select the receiver's status from the pulldown menu:

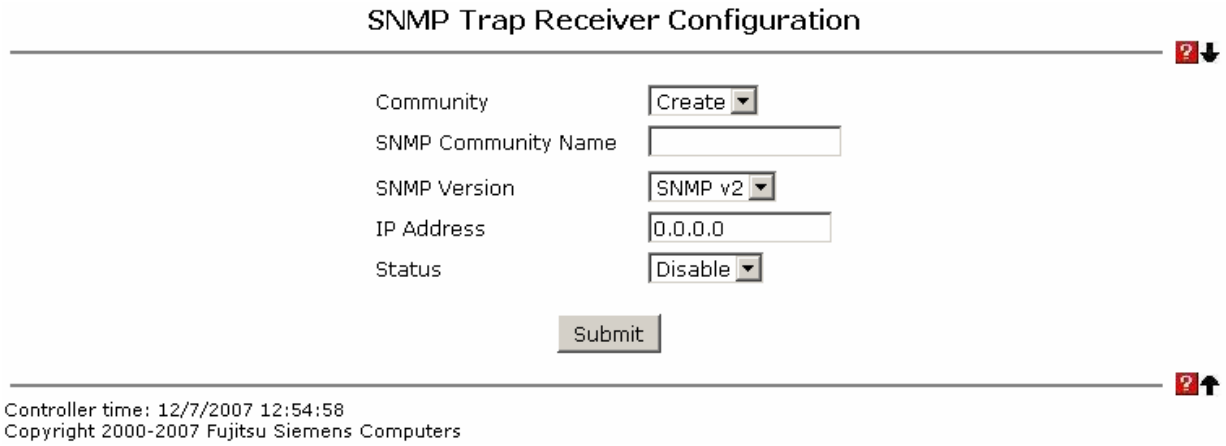
Enable - send traps to the receiver.

Disable - do not send traps to the receiver.

### Command Buttons

**Submit** - Update the IBP with the values on this screen. If you want the IBP to retain the new values across a power cycle, you must perform a save.

**Delete** - Delete the currently selected Community Name. If you want the IBP to retain the new values across a power cycle, you must perform a save.




**Viewing SNMP supported MIBs Page**

This is a list of all the MIBs supported by the IBP module.

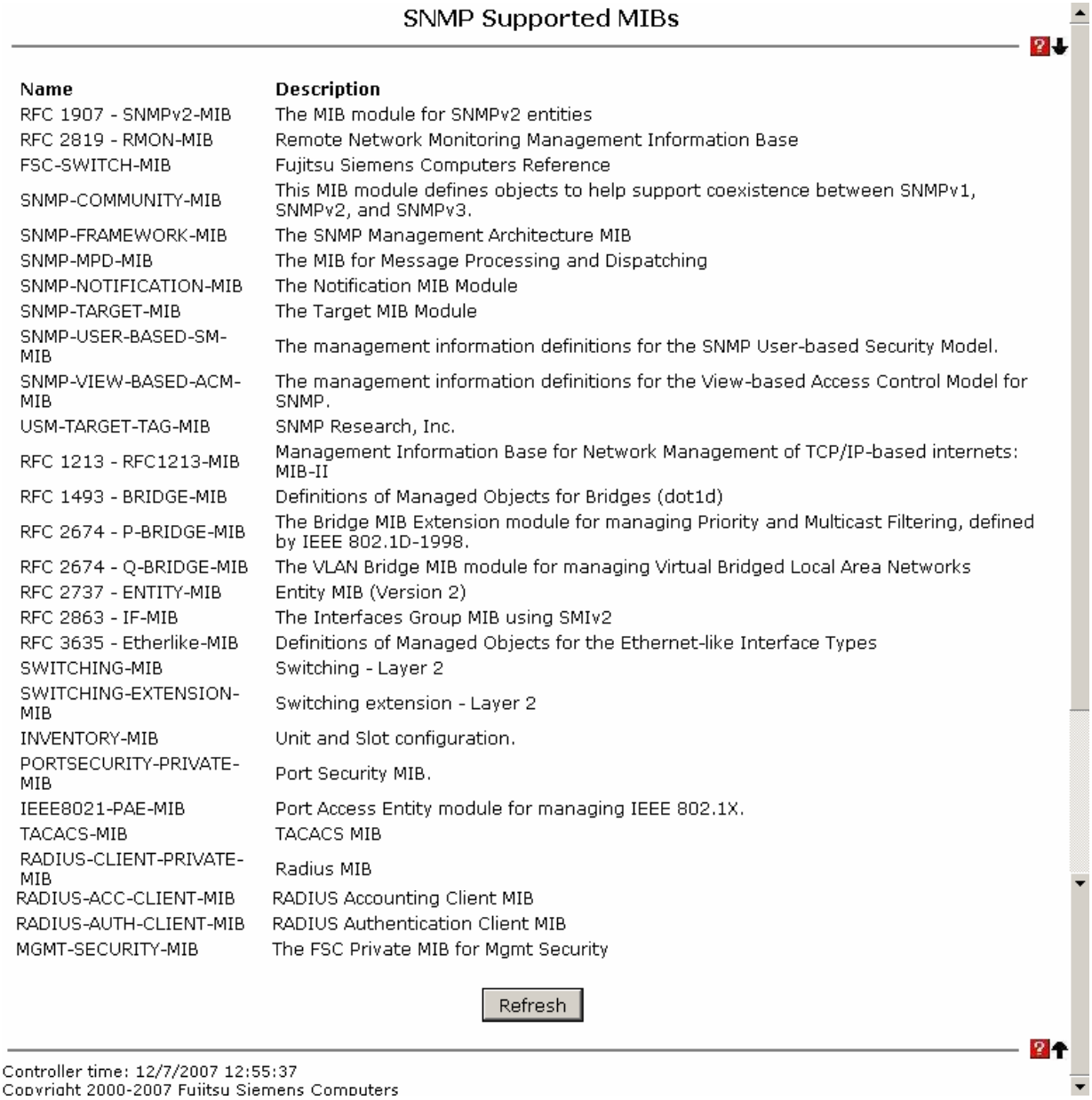
**Non-configurable Data**

**Name** - The RFC number if applicable and the name of the MIB.

**Description** - The RFC title or MIB description.

**Command Buttons**

**Refresh** - Update the data.



SNMP Supported MIBs

| Name | Description |
|---|---|
| RFC 1907 - SNMPv2-MIB | The MIB module for SNMPv2 entities |
| RFC 2819 - RMON-MIB | Remote Network Monitoring Management Information Base |
| FSC-SWITCH-MIB | Fujitsu Siemens Computers Reference |
| SNMP-COMMUNITY-MIB | This MIB module defines objects to help support coexistence between SNMPv1, SNMPv2, and SNMPv3. |
| SNMP-FRAMEWORK-MIB | The SNMP Management Architecture MIB |
| SNMP-MPD-MIB | The MIB for Message Processing and Dispatching |
| SNMP-NOTIFICATION-MIB | The Notification MIB Module |
| SNMP-TARGET-MIB | The Target MIB Module |
| SNMP-USER-BASED-SM-MIB | The management information definitions for the SNMP User-based Security Model. |
| SNMP-VIEW-BASED-ACM-MIB | The management information definitions for the View-based Access Control Model for SNMP. |
| USM-TARGET-TAG-MIB | SNMP Research, Inc. |
| RFC 1213 - RFC1213-MIB | Management Information Base for Network Management of TCP/IP-based internets: MIB-II |
| RFC 1493 - BRIDGE-MIB | Definitions of Managed Objects for Bridges (dot1d) |
| RFC 2674 - P-BRIDGE-MIB | The Bridge MIB Extension module for managing Priority and Multicast Filtering, defined by IEEE 802.1D-1998. |
| RFC 2674 - Q-BRIDGE-MIB | The VLAN Bridge MIB module for managing Virtual Bridged Local Area Networks |
| RFC 2737 - ENTITY-MIB | Entity MIB (Version 2) |
| RFC 2863 - IF-MIB | The Interfaces Group MIB using SMIv2 |
| RFC 3635 - Etherlike-MIB | Definitions of Managed Objects for the Ethernet-like Interface Types |
| SWITCHING-MIB | Switching - Layer 2 |
| SWITCHING-EXTENSION-MIB | Switching extension - Layer 2 |
| INVENTORY-MIB | Unit and Slot configuration. |
| PORTSECURITY-PRIVATE-MIB | Port Security MIB. |
| IEEE8021-PAE-MIB | Port Access Entity module for managing IEEE 802.1X. |
| TACACS-MIB | TACACS MIB |
| RADIUS-CLIENT-PRIVATE-MIB | Radius MIB |
| RADIUS-ACC-CLIENT-MIB | RADIUS Accounting Client MIB |
| RADIUS-AUTH-CLIENT-MIB | RADIUS Authentication Client MIB |
| MGMT-SECURITY-MIB | The FSC Private MIB for Mgmt Security |

Refresh

Controller time: 12/7/2007 12:55:37
Copyright 2000-2007 Fujitsu Siemens Computers

#### 6.2.2.1.10 Configuring SNTP

**Configuring SNTP Global Configuration Page**

**Configurable Data**

**Client Mode** - Specifies the mode of operation of SNTP Client. An SNTP client may operate in one of the following modes.

- ***Disable***- SNTP is not operational. No SNTP requests are sent from the client nor are any received SNTP messages processed.
- ***Unicast***- SNTP operates in a point to point fashion. A unicast client sends a request to a designated server at its unicast address and expects a reply from which it can determine the time and, optionally the round-trip delay and local clock offset relative to the server.
- ***Broadcast*** - SNTP operates in the same manner as multicast mode but uses a local broadcast address instead of a multicast address. The broadcast address has a single subnet scope while a multicast address has Internet wide scope. Default value is Disable.

**Port** - Specifies the local UDP port to listen for responses/broadcasts. Allowed range is (1 to 65535). Default value is 123.

**Unicast Poll Interval** - Specifies the number of seconds between unicast poll requests expressed as a power of two when configured in unicast mode. Allowed range is (6 to 10). Default value is 6.

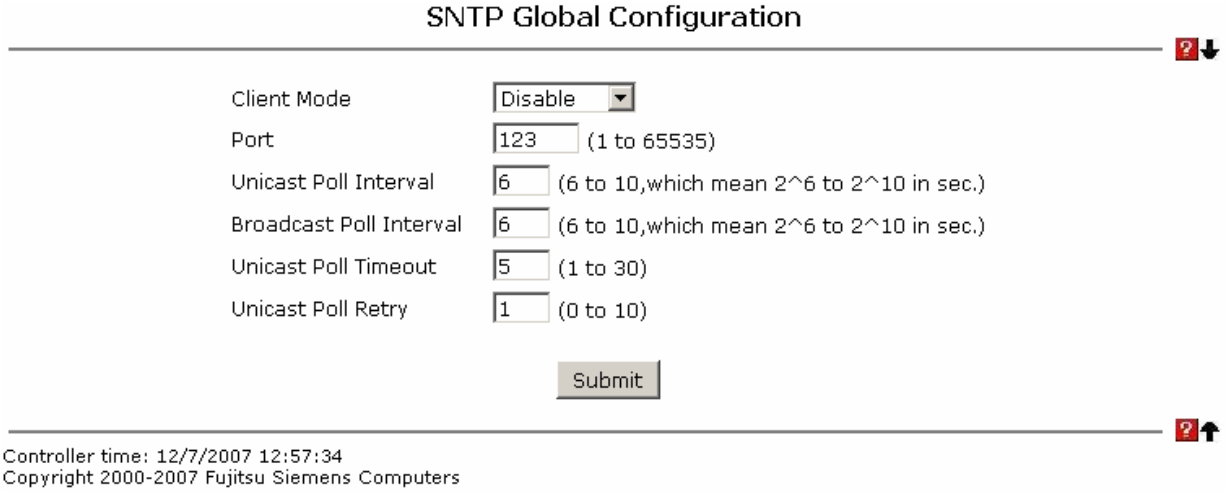
**Broadcast Poll Interval** - Specifies the number of seconds between broadcast poll requests expressed as a power of two when configured in broadcast mode. Broadcasts received prior to the expiry of this interval are discarded. Allowed range is (6 to 10). Default value is 6.

**Unicast Poll Timeout** - Specifies the number of seconds to wait for an SNTP response when configured in unicast mode. Allowed range is (1 to 30). Default value is 5.

**Unicast Poll Retry** - Specifies the number of times to retry a request to an SNTP server after the first time-out before attempting to use the next configured server when configured in unicast mode. Allowed range is (0 to 10). Default value is 1.

**Command Buttons**

**Submit** - Sends the updated configuration to the IBP. Configuration changes take effect immediately.




**Viewing SNTP Global Status Page**

**Non-Configurable Data**

**Version** - Specifies the SNTP Version the client supports.

**Supported Mode** - Specifies the SNTP modes the client supports. Multiple modes may be supported by a client.

**Last Update Time** - Specifies the local date and time (UTC) the SNTP client last updated the system clock.

**Last Attempt Time** - Specifies the local date and time (UTC) of the last SNTP request or receipt of an unsolicited message.

**Last Attempt Status** - Specifies the status of the last SNTP request or unsolicited message for both unicast and broadcast modes. If no message has been received from a server, a status of Other is displayed. These values are appropriate for all operational modes.

- ***Other*** None of the following enumeration values.
- ***Success***The SNTP operation was successful and the system time was updated.
- ***Request Timed Out*** A directed SNTP request timed out without receiving a response from the SNTP server.
- ***Bad Date Encoded*** The time provided by the SNTP server is not valid.
- ***Version Not Supported*** TheSNTP version supported by the server is not compatible with the version supported by the client.
- ***Server Unsychronized*** The SNTP server is not synchronized with its peers. This is indicated via the 'leap indicator' field on the SNTP message.
- ***Server Kiss Of Death*** The SNTP server indicated that no further queries were to be sent to this server. This is indicated by a stratum field equal to 0 in a message received from a server.

**Server IP Address** - Specifies the IP address of the server for the last received valid packet. If no message has been received from any server, an empty string is shown.

**Address Type** - Specifies the address type of the SNTP Server address for the last received valid packet.

**Server Stratum** - Specifies the claimed stratum of the server for the last received valid packet.

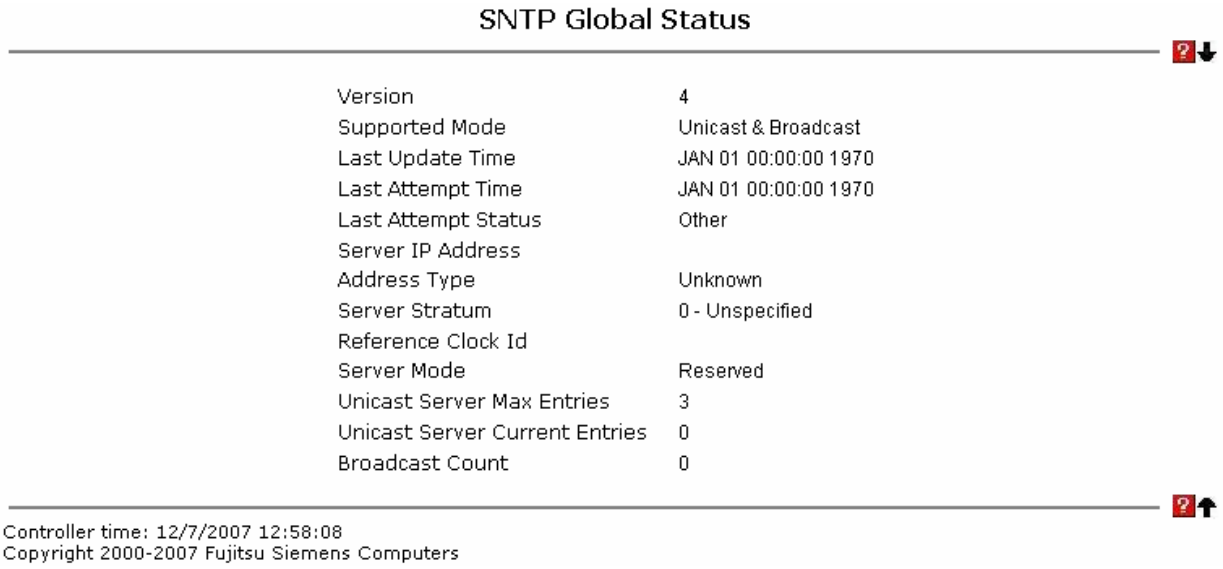
**Reference Clock Id** - Specifies the reference clock identifier of the server for the last received valid packet.

**Server Mode** - Specifies the mode of the server for the last received valid packet.

**Unicast Sever Max Entries** - Specifies the maximum number of unicast server entries that can be configured on this client.

**Unicast Server Current Entries** - Specifies the number of current valid unicast server entries configured for this client.

**Broadcast Count** - Specifies the number of unsolicited broadcast SNTP messages that have been received and processed by the SNTP client since last reboot.


SNTP Global Status
Version 4
Supported Mode Unicast & Broadcast
Last Update Time JAN 01 00:00:00 1970
Last Attempt Time JAN 01 00:00:00 1970
Last Attempt Status Other
Server IP Address
Address Type Unknown
Server Stratum 0 - Unspecified
Reference Clock Id
Server Mode Reserved
Unicast Server Max Entries 3
Unicast Server Current Entries 0
Broadcast Count 0
Controller time: 12/7/2007 12:58:08
Copyright 2000-2007 Fujitsu Siemens Computers

### Configuring SNTP Server Configuration Page

### Configurable Data

**Server** - Specifies all the existing Server Addresses along with an additional option "Create". When the user selects "Create" another text box "Address" appears where the user may enter Address for Server to be configured.

**Address** - Specifies the address of the SNTP server. This is a text string of up to 64 characters containing the encoded unicast IP address or hostname of a SNTP server. Unicast SNTP requests will be sent to this address.

**Address Type** - Specifies the address type of the configured SNTP Server address.

Allowed types are :

- ***Unknown***
- ***IPV4***

Default value is Unknown

**Port** - Specifies the port on the server to which SNTP requests are to be sent. Allowed range is (1 to 65535). Default value is 123.

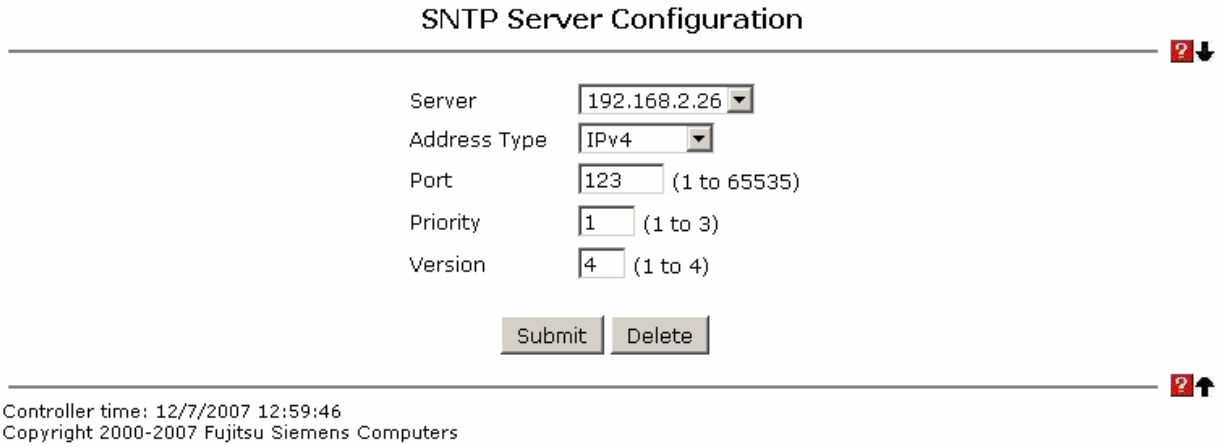
**Priority** - Specifies the priority of this server entry in determining the sequence of servers to which SNTP requests will be sent. The client continues sending requests to different servers until a successful response is received or all servers are exhausted. This object indicates the order in which to query the servers. A server entry with a precedence of 1 will be queried before a server with a priority of 2, and so forth. If more than one server has the same priority then the requesting order will follow the lexicographical ordering of the entries in this table. Allowed range is (1 to 3). Default value is 1.

**Version** - Specifies the NTP Version running on the server. Allowed range is (1 to 4). Default value is 4.

### Command Buttons

**Submit** - Sends the updated configuration to the IBP. Configuration changes take effect immediately.

**Delete** - Deletes the SNTP Server entry. Sends the updated configuration to the IBP Configuration changes take effect immediately.




### Viewing SNTP Server Status Page

### Non-Configurable Data

**Address** - Specifies all the existing Server Addresses. If no Server configuration exists, a message saying "No SNTP server exists" flashes on the screen.

**Last Update Time** - Specifies the local date and time (UTC) that the response from this server was used to update the system clock.

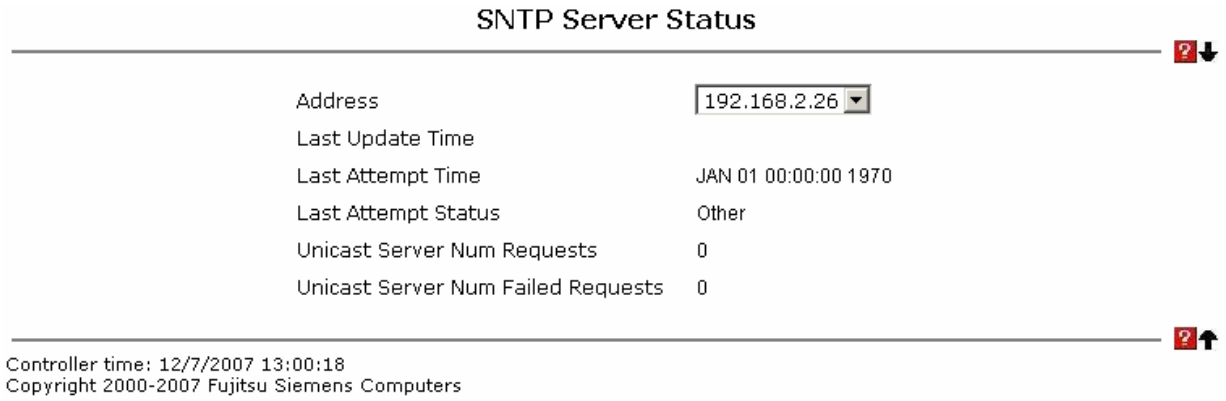
**Last Attempt Time** - Specifies the local date and time (UTC) that this SNTP server was last queried.

**Last Attempt Status** - Specifies the status of the last SNTP request to this server. If no packet has been received from this server, a status of Other is displayed.

- ***Other*** None of the following enumeration values.
- ***Success*** The SNTP operation was successful and the system time was updated.
- ***Request Timed Out*** A directed SNTP request timed out without receiving a response from the SNTP server.
- ***Bad Date Encoded*** The time provided by the SNTP server is not valid.
- ***Version Not Supported*** TheSNTP version supported by the server is not compatible with the version supported by the client.
- ***Server Unsychronized***The SNTP server is not synchronized with its peers. This is indicated via the 'leap indicator' field on the SNTP message.
- ***Server Kiss Of Death*** The SNTP server indicated that no further queries were to be sent to this server. This is indicated by a stratum field equal to 0 in a message received from a server.

**Unicast Server Num Requests** - Specifies the number of SNTP requests made to this server since last time agent reboot.

**Unicast Server Num Failed Requests** - Specifies the number of failed SNTP requests made to this server since last reboot.



### 6.2.2.2 Configuring IBP Interface

#### 6.2.2.2.1 Interface Configuration Page

**Selection Criteria**

**Slot/Port** - Selects the interface for which data is to be displayed or configured.

**Configurable Data**

**Physical Mode** - Use the pulldown menu to select the port's speed and duplex mode. If you select auto the duplex mode and speed will be set by the auto-negotiation process. Note that the port's maximum capability (full duplex and 100 Mbps) will be advertised. Otherwise, your selection will determine the port's duplex mode and transmission rate. The factory default is auto. The selection when applied against the "All" option in Slot/Port is applied to all applicable interfaces only.

**Link Trap** - This object determines whether or not to send a trap when link status changes. The factory default is enabled.

**Maximum Frame Size** - The maximum Ethernet frame size the interface supports or is configured, including Ethernet header, CRC, and payload. (1518 to 9216). The default maximum frame size is 1518 . (Notes: If you configure an external port, the other external members of the same port group will be changed together.)

**Flow Control** - Used to enable or disable flow control feature on the selected interface.

**Capability** - You could advertise the port capabilities of a given interface during auto-negotiation.

**Port Description** – You can specify the description for this port.

**Non-Configurable Data**

**Port Type** - For normal ports this field will be blank. Otherwise the possible values are:

Mon - the port is a monitoring port. Look at the Port Monitoring screens for more information.

LAG - the port is a member of a Link Aggregation trunk. Look at the LAG screens for more information.

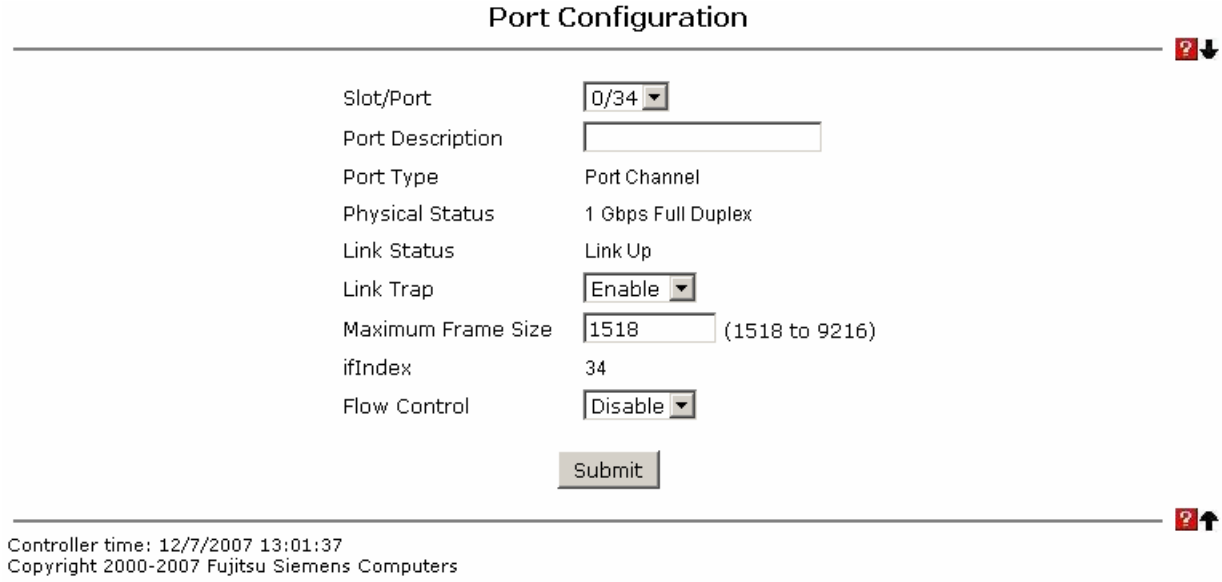
**Physical Status** - Indicates the port speed and duplex mode.

**Link Status** - Indicates whether the Link is up or down.

**ifIndex** - The ifIndex of the interface table entry associated with this port.

**Command Buttons**

**Submit** - Update the IBP module with the values you entered. If you want the IBP module to retain the new values across a power cycle you must perform a save.




#### 6.2.2.2.2 Viewing Interface Configuration Page

This screen displays the status for all ports in the box.

**Non-Configurable Port Status Data**

**Slot/Port** - Identifies the port

**Port Type** - For normal ports this field will be blank. Otherwise the possible values are:

Mon - this port is a monitoring port. Look at the Port Monitoring screens for more information.

LAG - the port is a member of a Link Aggregation trunk. Look at the LAG screens for more information.

**Forwarding State** - The port's current state Spanning Tree state. This state controls what action a port takes on receipt of a frame. If the bridge detects a malfunctioning port it will place that port into the broken state. The possible states are Disabled, Blocking, and Manual Forwarding.

**Admin Mode** - The Port control administration state. The port must be enabled in order for it to be allowed into the network. The factory default is enabled.

**Physical Mode** - Indicates the port speed and duplex mode. In auto-negotiation mode the duplex mode and speed are set from the auto-negotiation process.

**Physical Status** - Indicates the port speed and duplex mode.

**Link Status** - Indicates whether the Link is up or down.

**Link Trap** - Indicates whether or not the port will send a trap when link status changes.

**ifIndex** - Indicates the ifIndex of the interface table entry associated with this port.

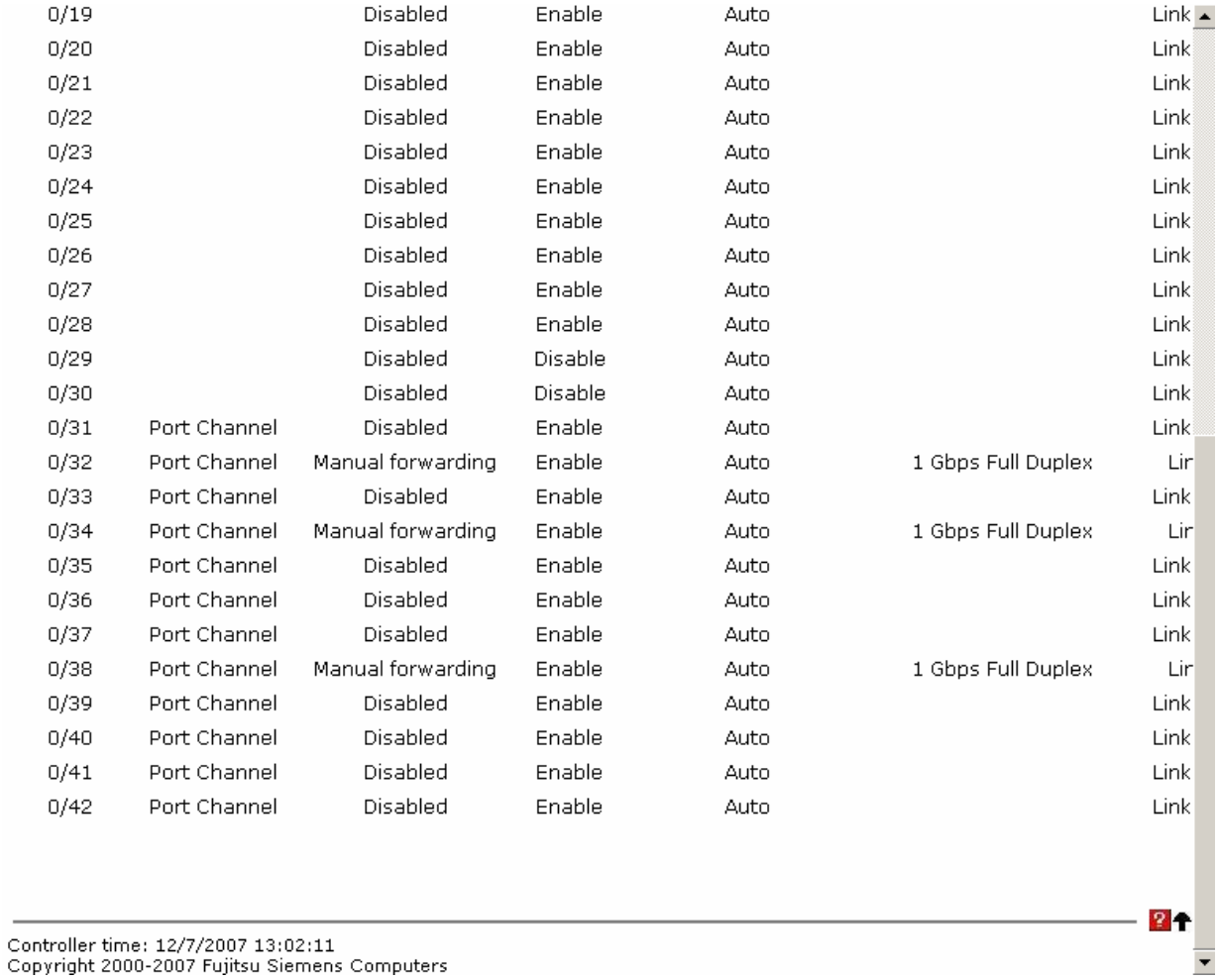
**Flow Control** - Indicates the status of flow control on this port.

**Capability** - Indicates the port capabilities during auto-negotiation.

**Port Description** – the description for this port.

**Command Buttons**

**Refresh** – Refresh the configuration value again.



| | | | | | | |
|---|---|---|---|---|---|---|
| 0/19 | | Disabled | Enable | Auto | | Link |
| 0/20 | | Disabled | Enable | Auto | | Link |
| 0/21 | | Disabled | Enable | Auto | | Link |
| 0/22 | | Disabled | Enable | Auto | | Link |
| 0/23 | | Disabled | Enable | Auto | | Link |
| 0/24 | | Disabled | Enable | Auto | | Link |
| 0/25 | | Disabled | Enable | Auto | | Link |
| 0/26 | | Disabled | Enable | Auto | | Link |
| 0/27 | | Disabled | Enable | Auto | | Link |
| 0/28 | | Disabled | Enable | Auto | | Link |
| 0/29 | | Disabled | Disable | Auto | | Link |
| 0/30 | | Disabled | Disable | Auto | | Link |
| 0/31 | Port Channel | Disabled | Enable | Auto | | Link |
| 0/32 | Port Channel | Manual forwarding | Enable | Auto | 1 Gbps Full Duplex | Lir |
| 0/33 | Port Channel | Disabled | Enable | Auto | | Link |
| 0/34 | Port Channel | Manual forwarding | Enable | Auto | 1 Gbps Full Duplex | Lir |
| 0/35 | Port Channel | Disabled | Enable | Auto | | Link |
| 0/36 | Port Channel | Disabled | Enable | Auto | | Link |
| 0/37 | Port Channel | Disabled | Enable | Auto | | Link |
| 0/38 | Port Channel | Manual forwarding | Enable | Auto | 1 Gbps Full Duplex | Lir |
| 0/39 | Port Channel | Disabled | Enable | Auto | | Link |
| 0/40 | Port Channel | Disabled | Enable | Auto | | Link |
| 0/41 | Port Channel | Disabled | Enable | Auto | | Link |
| 0/42 | Port Channel | Disabled | Enable | Auto | | Link |

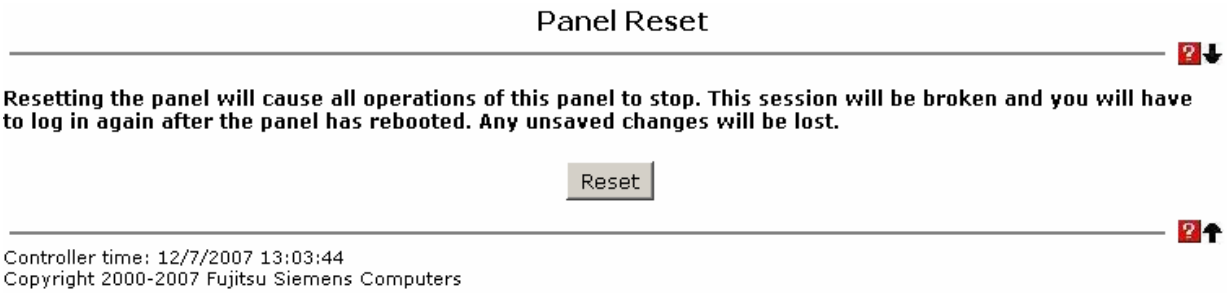
Controller time: 12/7/2007 13:02:11
Copyright 2000-2007 Fujitsu Siemens Computers

### 6.2.2.3 Managing System Utilities

#### 6.2.2.3.1 Panel Reset Page

**Command Buttons**

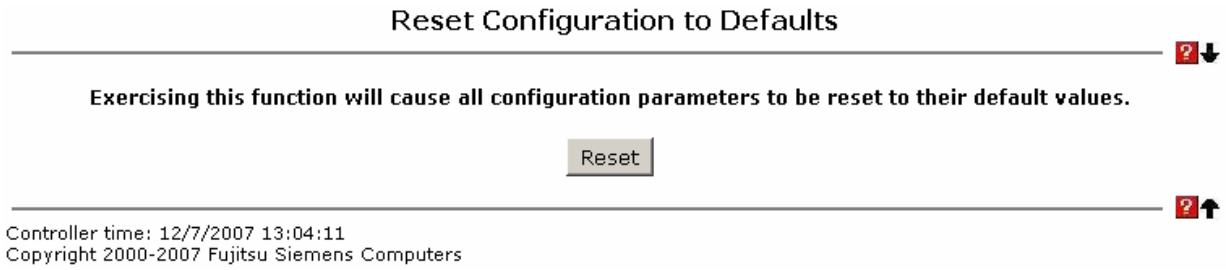
**Reset** - Select this button to reboot the IBP. Any configuration changes you have made since the last time you issued a save will be lost. You will be shown a confirmation screen after you select the button.


Panel Reset
Resetting the panel will cause all operations of this panel to stop. This session will be broken and you will have to log in again after the panel has rebooted. Any unsaved changes will be lost.
Reset
Controller time: 12/7/2007 13:03:44
Copyright 2000-2007 Fujitsu Siemens Computers

#### 6.2.2.3.2 Reset All Configuration to Defaults Page

**Command Buttons**

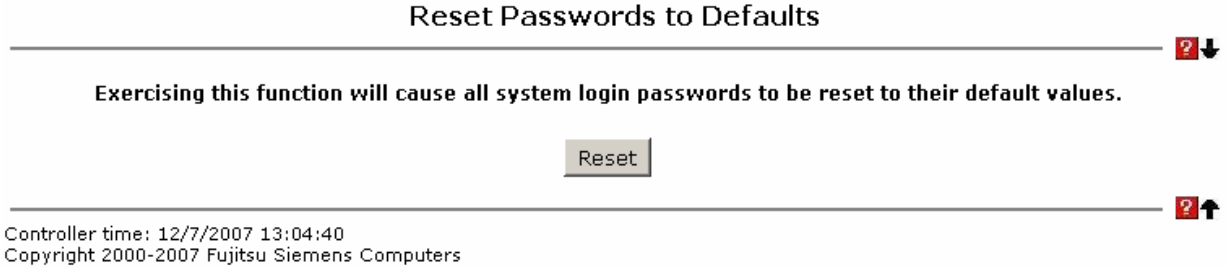
**Reset** - Clicking the Reset button will reset all of the system login passwords to their default values. If you want the IBP to retain the new values across a power cycle, you must perform a save.


Reset Configuration to Defaults
Exercising this function will cause all configuration parameters to be reset to their default values.
Reset
Controller time: 12/7/2007 13:04:11
Copyright 2000-2007 Fujitsu Siemens Computers

#### 6.2.2.3.3 Reset the Passwords to Defaults Page

**Command Buttons**

**Reset** - Select this button to have all passwords reset to their factory default values.


Reset Passwords to Defaults
Exercising this function will cause all system login passwords to be reset to their default values.
Reset
Controller time: 12/7/2007 13:04:40
Copyright 2000-2007 Fujitsu Siemens Computers

#### 6.2.2.3.4 Downloading Specific Files to Panel Page

Use this menu to download a file to the Panel.

**Configurable Data**

**File Type** - Specify what type of file you want to download:

**Script** - specify configuration script when you want to update the IBP's script file.

**CLI Banner** - Specify the banner that you want to display before user login to the IBP.

**Code** – Specify code when you want to upgrade the operational flash.

**Configuration** - Specify configuration when you want to update the IBP's configuration. If the file has errors the update will be stopped.

**SSH-1 RSA Key File** - SSH-1 Rivest-Shamir-Adleman (RSA) Key File

**SSH-2 RSA Key PEM File** - SSH-2 Rivest-Shamir-Adleman (RSA) Key File (PEM Encoded)

**SSH-2 DSA Key PEM File** - SSH-2 Digital Signature Algorithm (DSA) Key File (PEM Encoded)

**SSL Trusted Root Certificate PEM File** - SSL Trusted Root Certificate File (PEM Encoded)

**SSL Server Certificate PEM File** - SSL Server Certificate File (PEM Encoded)

**SSL DH Weak Encryption Parameter PEM File** - SSL Diffie-Hellman Weak Encryption Parameter File (PEM Encoded)

**SSL DH Strong Encryption Parameter PEM File** - SSL Diffie-Hellman Strong Encryption Parameter File (PEM Encoded)

The factory default is code.
Note that to download SSH key files SSH must be administratively disabled and there can be no active SSH sessions.

**TFTP Server IP Address** - Enter the IP address of the TFTP server. The factory default is 0.0.0.0.

**TFTP File Path (Target)** - Enter the path on the TFTP server where the selected file is located. You may enter up to 32 characters. The factory default is blank.

**TFTP File Name (Source)** - Enter the name on the TFTP server of the file you want to download. You may enter up to 32 characters. The factory default is blank.

**TFTP File Name (Target)** - Enter the name on the IBP of the file you want to save. You may enter up to 32 characters. The factory default is blank.

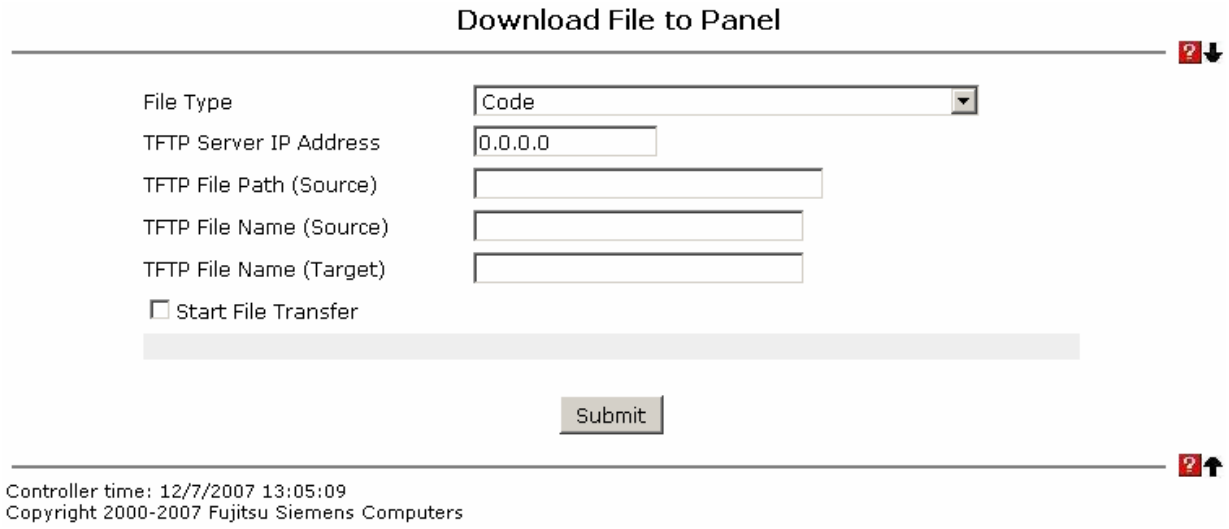
**Start File Transfer** - To initiate the download you need to check this box and then select the submit button.

**Non-Configurable Data**

The last row of the table is used to display information about the progress of the file transfer. The screen will refresh automatically until the file transfer completes.

**Command Buttons**

**Submit** - Send the updated screen to the IBP and perform the file download.




#### 6.2.2.3.5 Uploading Specific Files from Panel Page

Use this menu to upload a code, configuration, or log file from the IBP.

**Configurable Data**

**File Type** - Specify the type of file you want to upload. The available options are Script, Code, CLI Banner, Configuration, Error Log, Buffered Log, and Trap Log. The factory default is Error Log.

**TFTP Server IP Address** - Enter the IP address of the TFTP server. The factory default is 0.0.0.0

**TFTP File Path (Target)** - Enter the path on the TFTP server where you want to put the file being uploaded. You may enter up to 32 characters. The factory default is blank.

**TFTP File Name (Target)** - Enter the name you want to give the file being uploaded. You may enter up to 32 characters. The factory default is blank.

**TFTP File Name (Source)** - Specify the file which you want to upload from the IBP.

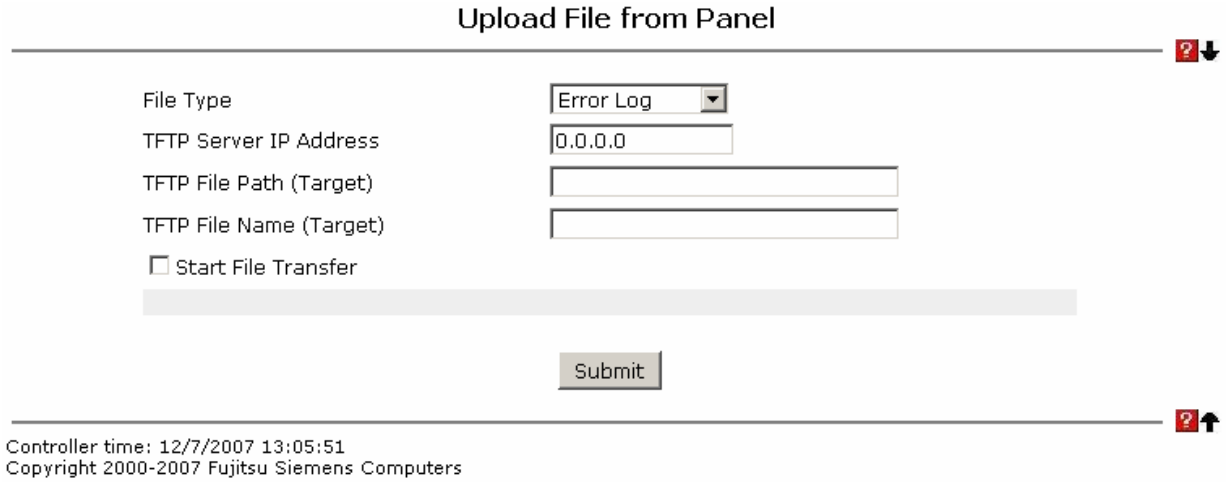
**Start File Transfer** - To initiate the upload you need to check this box and then select the submit button.

**Non-Configurable Data**

The last row of the table is used to display information about the progress of the file transfer. The screen will refresh automatically until the file transfer completes.

**Command Buttons**

**Submit** - Send the updated screen to the IBP and perform the file upload.




#### 6.2.2.3.6 Defining Configuration and Runtime Startup File Page

Specify the file used to start up the system.

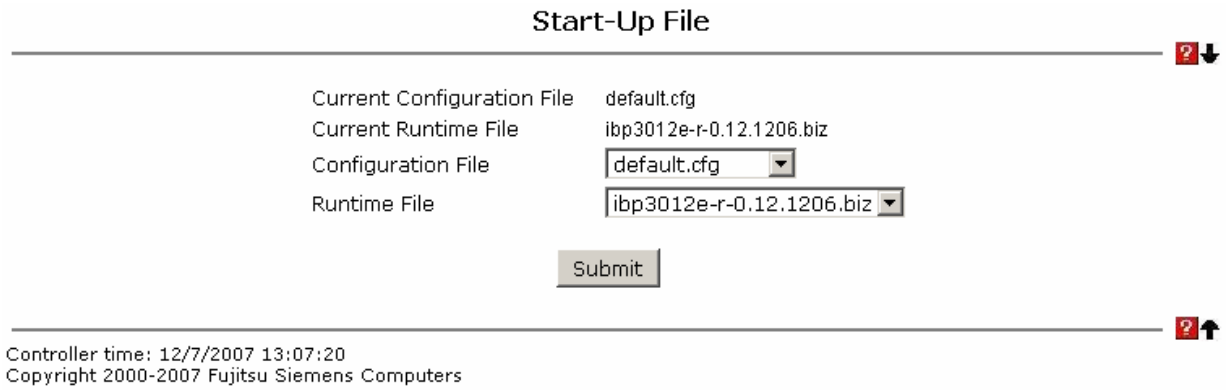
**Configurable Data**

**Configuration File** - Configuration files.

**Runtime File** - Run-time operation codes.

**Command Buttons**

**Submit** - Send the updated screen to the IBP and specify the file start-up.




#### 6.2.2.3.7 Removing Specific File Page

Delete files in flash. If the file type is used for system startup, then this file cannot be deleted.

**Configurable Data**

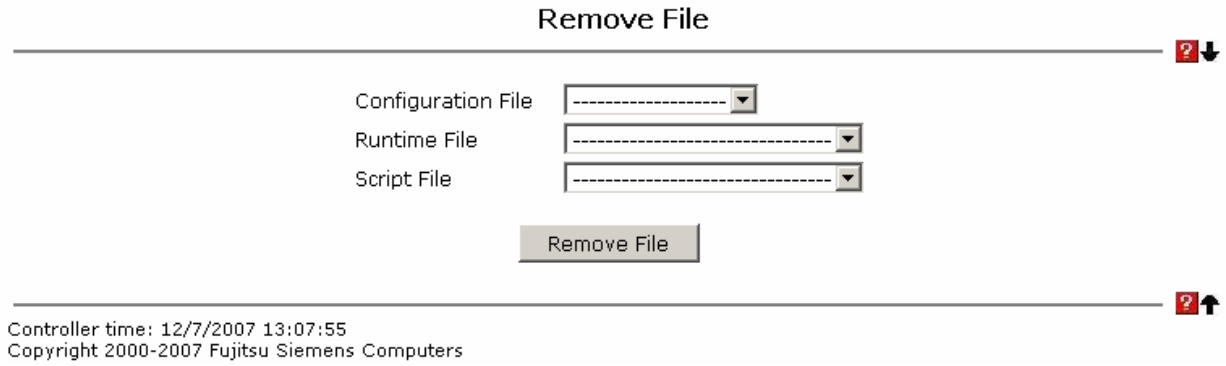
**Configuration File** - Configuration files.

**Runtime File** - Run-time operation codes.

**Script File** - Configuration script files.

**Command Buttons**

**Remove File** - Send the updated screen to the IBP and perform the file remove.




#### 6.2.2.3.8 Copying Running Configuration to Panel Page

Use this menu to copy a start-up configuration file from the running configuration file on IBP.

**Configurable Data**

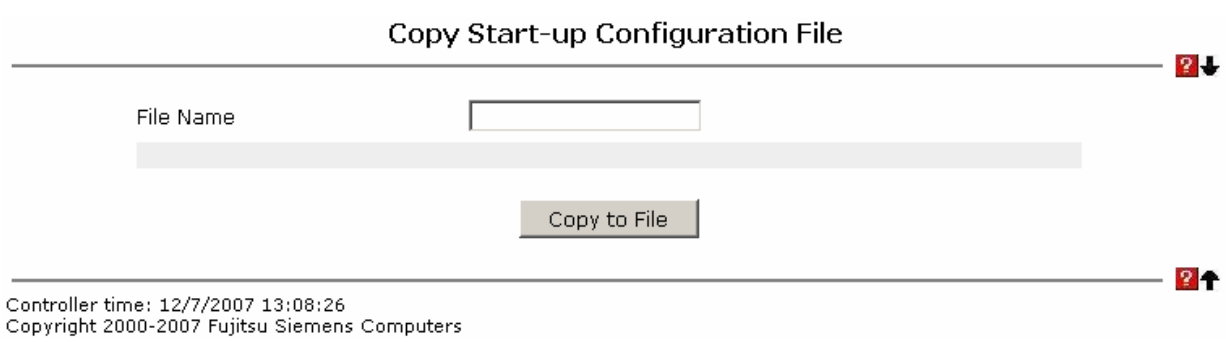
**File Name** - Enter the name you want to give the file being copied. You may enter up to 32 characters. The factory default is blank.

**Non-Configurable Data**

The last row of the table is used to display information about the progress of the file copy. The screen will refresh automatically until the file copy completes.

**Command Buttons**

**Copy to File** - Send the updated screen to the IBP perform the file copy.




#### 6.2.2.3.9 Defining Ping Function Page

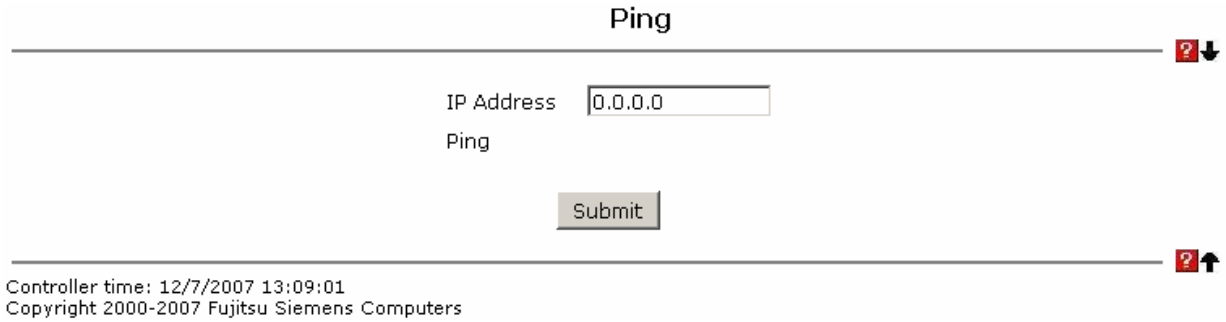
Use this screen to tell the IBP to send a Ping request to a specified IP address. You can use this to check whether the IBP can communicate with a particular IP station. Once you click the Submit button, the IBP will send three pings and the results will be displayed below the configurable data. If a reply to the ping is not received, you will see **No Reply Received from IP xxx.xxx.xxx.xxx**, otherwise you will see **Reply received from IP xxx.xxx.xxx.xxx : (send count = 5, receive count = n).**

**Configurable Data**

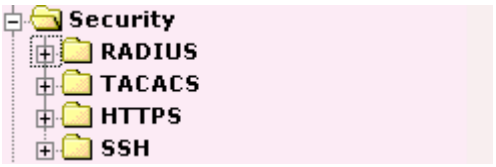
**IP Address** - Enter the IP address of the station you want the IBP to ping. The initial value is blank. The IP Address you enter is not retained across a power cycle.

### Command Buttons

**Submit** - This will initiate the ping.



### 6.2.3 Security Menu




#### 6.2.3.1 Managing RADIUS

##### 6.2.3.1.1 Configuring RADIUS Configuration Page

**Configurable Data**

**Max Number of Retransmits** - The value of the maximum number of times a request packet is retransmitted. The valid range is 1 - 15. Consideration to maximum delay time should be given when configuring RADIUS maxretransmit and RADIUS timeout. If multiple RADIUS servers are configured, the max retransmit value on each will be exhausted before the next server is attempted. A retransmit will not occur until the configured timeout value on that server has passed without a response from the RADIUS server. Therefore, the maximum delay in receiving a response from the RADIUS application equals the sum of (retransmit times timeout) for all configured servers. If the RADIUS request was generated by a user login attempt, all user interfaces will be blocked until the RADIUS application returns a response.

**Timeout Duration (secs)** - The timeout value, in seconds, for request retransmissions. The valid range is 1 - 30. Consideration to maximum delay time should be given when configuring RADIUS maxretransmit and RADIUS timeout. If multiple RADIUS servers are configured, the max retransmit value on each will be exhausted before the next server is attempted. A retransmit will not occur until the configured timeout value on that server has passed without a response from the RADIUS server. Therefore, the maximum delay in receiving a response from the RADIUS application equals the sum of (retransmit times timeout) for all configured servers. If the RADIUS request was generated by a user login attempt, all user interfaces will be blocked until the RADIUS application returns a response.

**Accounting Mode** - Selects if the RADIUS accounting mode is enabled or disabled.

**Non-Configurable Data**

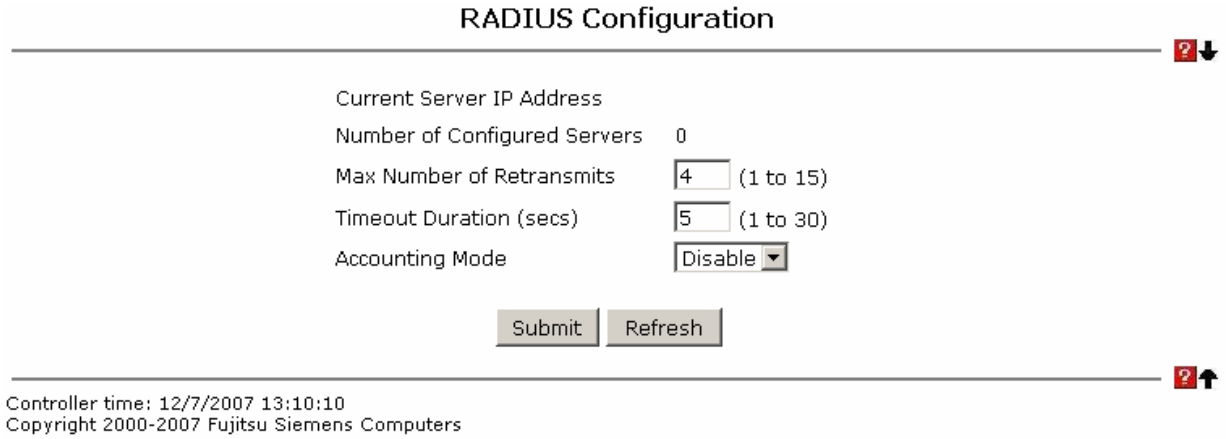
**Current Server IP Address** - The IP address of the current server. This field is blank if no servers are configured.

**Number of Configured Servers** - The number of RADIUS servers that have been configured. This value will be in the range of 0 and 3.

**Command Buttons**

**Submit** - Sends the updated screen to the IBP and causes the changes to take effect on the IBP but these changes will not be retained across a power cycle unless a save is performed.

**Refresh** - Update the information on the page.


RADIUS Configuration
Current Server IP Address
Number of Configured Servers 0
Max Number of Retransmits 4 (1 to 15)
Timeout Duration (secs) 5 (1 to 30)
Accounting Mode Disable
Submit
Refresh
Controller time: 12/7/2007 13:10:10
Copyright 2000-2007 Fujitsu Siemens Computers

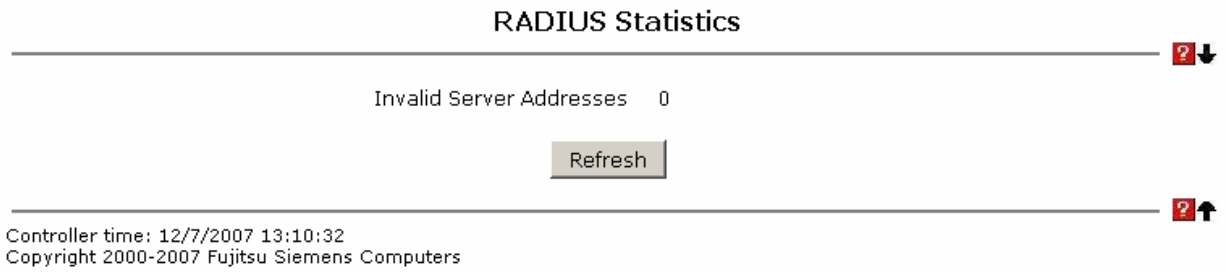
#### 6.2.3.1.2 Viewing Radius Statistics Page

**Non-Configurable Data**

**Invalid Server Addresses** - The number of RADIUS Access-Response packets received from unknown addresses.

**Command Buttons**

**Refresh** - Update the information on the page.




#### 6.2.3.1.3 Configuring RADIUS Server Configuration Page

**Selection Criteria**

**RADIUS Server IP Address** - Selects the RADIUS server to be configured. Select add to add a server.

**Configurable Data**

**IP Address** - The IP address of the server being added.

**Port** - The UDP port used by this server. The valid range is 0 - 65535.

**Secret** - The shared secret for this server. This is an input field only.

**Apply** - The Secret will only be applied if this box is checked. If the box is not checked, anything entered in the Secret field will have no affect and will not be retained. This field is only displayed if the user has READWRITE access.

**Primary Server** - Sets the selected server to the Primary or Secondary server.

**Message Authenticator** - Enable or disable the message authenticator attribute for the selected server.

**Non-Configurable Data**

**Current** - Indicates if this server is currently in use as the authentication server.

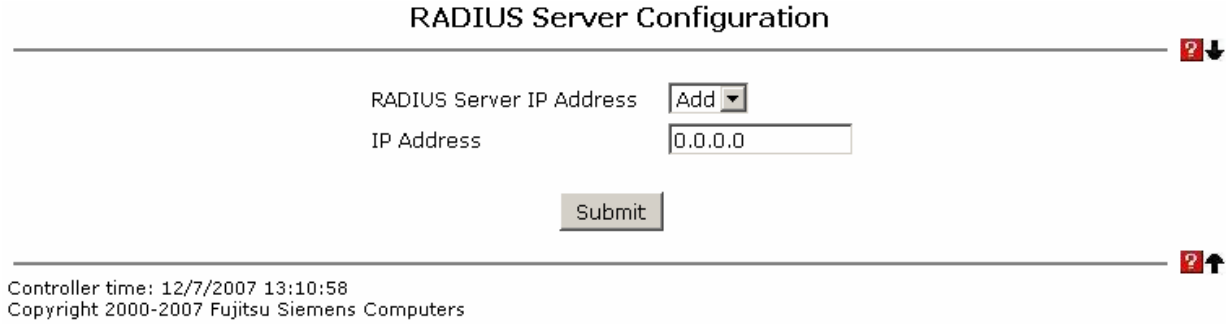
**Secret Configured** - Indicates if the shared secret for this server has been configured.

**Command Buttons**

**Submit** - Sends the updated screen to the IBP and causes the changes to take effect on the IBP but these changes will not be retained across a power cycle unless a save is performed.

**Remove** - Remove the selected server from the configuration. This button is only available to READWRITE users. These changes will not be retained across a power cycle unless a save is performed.

**Refresh** - Update the information on the page.




### 6.2.3.1.4 Viewing RADIUS Server Statistics Page

**Selection Criteria**

**RADIUS Server IP Address** - Selects the IP address of the RADIUS server for which to display statistics.

**Non-Configurable Data**

**Round Trip Time (secs)** - The time interval, in hundredths of a second, between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from this RADIUS authentication server.

**Access Requests** - The number of RADIUS Access-Request packets sent to this server. This number does not include retransmissions.

**Access Retransmissions** - The number of RADIUS Access-Request packets retransmitted to this server.

**Access Accepts** - The number of RADIUS Access-Accept packets, including both valid and invalid packets that were received from this server.

**Access Rejects** - The number of RADIUS Access-Reject packets, including both valid and invalid packets that were received from this server.

**Access Challenges** - The number of RADIUS Access-Challenge packets, including both valid and invalid packets that were received from this server.

**Malformed Access Responses** - The number of malformed RADIUS Access-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators or signature attributes or unknown types are not included as

malformed access-responses.

**Bad Authenticators** - The number of RADIUS Access-Response packets containing invalid authenticators or signature attributes received from this server.

**Pending Requests** - The number of RADIUS Access-Request packets destined for this server that have not yet timed out or received a response.

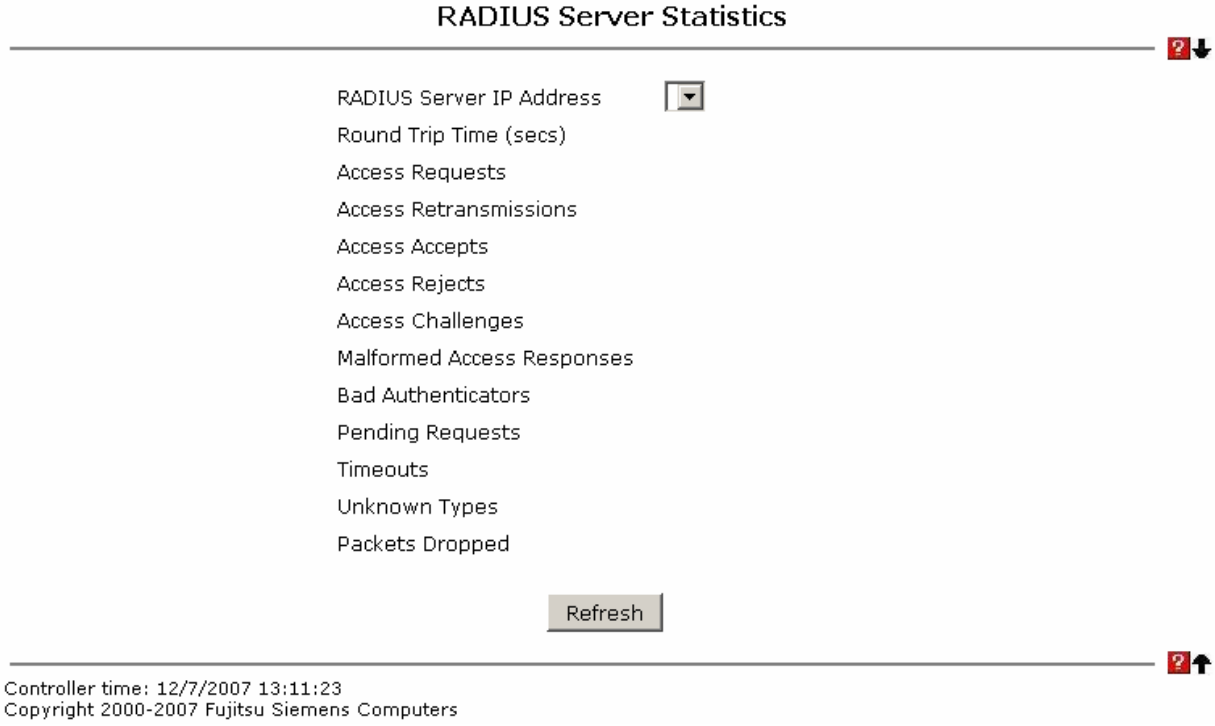
**Timeouts** - The number of authentication timeouts to this server.

**Unknown Types** - The number of RADIUS packets of unknown type which were received from this server on the authentication port.

**Packets Dropped** - The number of RADIUS packets received from this server on the authentication port and dropped for some other reason.

**Command Buttons**

**Refresh** - Update the information on the page.




### 6.2.3.1.5 Defining RADIUS Accounting Server Configuration Page

**Selection Criteria**

**Accounting Server IP Address** - Selects the accounting server for which data is to be displayed or configured. If the add item is selected, a new accounting server can be configured.

**Configurable Data**

**IP Address** - The IP address of the accounting server to add. This field is only configurable if the add item is selected.

**Port** - Specifies the UDP Port to be used by the accounting server. The valid range is 0 - 65535. If the user has READONLY access, the value is displayed but cannot be changed.

**Secret** - Specifies the shared secret to use with the specified accounting server. This field is only displayed if the user has READWRITE access.

**Apply** - The Secret will only be applied if this box is checked. If the box is not checked, anything entered in the Secret field will have no affect and will not be retained. This field is only displayed if the user has READWRITE access.

**Non-Configurable Data**

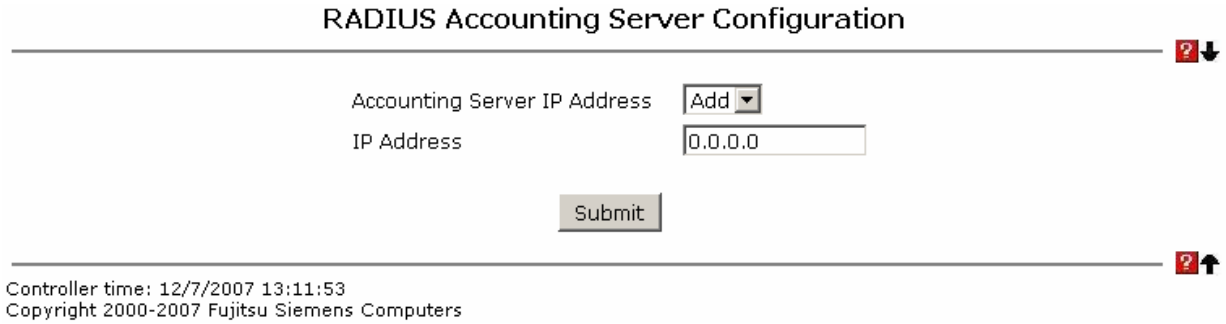
**Secret Configured** - Indicates if the secret has been configured for this accounting server.

**Command Buttons**

**Submit** - Sends the updated screen to the IBP and causes the changes to take effect on the IBP but these changes will not be retained across a power cycle unless a save is performed.

**Remove** - Remove the selected accounting server from the configuration. This button is only available to READWRITE users. These changes will not be retained across a power cycle unless a save is performed.

**Refresh** - Update the information on the page.




#### 6.2.3.1.6 Viewing RADIUS Accounting Server Statistics Page

**Non-Configurable Statistics**

**Accounting Server IP Address** - Identifies the accounting server associated with the statistics.

**Round Trip Time (secs)** - Displays the time interval, in hundredths of a second, between the most recent Accounting-Response and the Accounting-Request that matched it from this RADIUS accounting server.

**Accounting Requests** - Displays the number of RADIUS Accounting-Request packets sent not including retransmissions.

**Accounting Retransmissions** - Displays the number of RADIUS Accounting-Request packets retransmitted to this RADIUS accounting server.

**Accounting Responses** - Displays the number of RADIUS packets received on the accounting port from this server.

**Malformed Accounting Responses** - Displays the number of malformed RADIUS Accounting-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators and unknown types are not included as malformed accounting responses.

**Bad Authenticators** - Displays the number of RADIUS Accounting-Response packets

that contained invalid authenticators received from this accounting server.

**Pending Requests** - Displays the number of RADIUS Accounting-Request packets sent to this server that have not yet timed out or received a response.

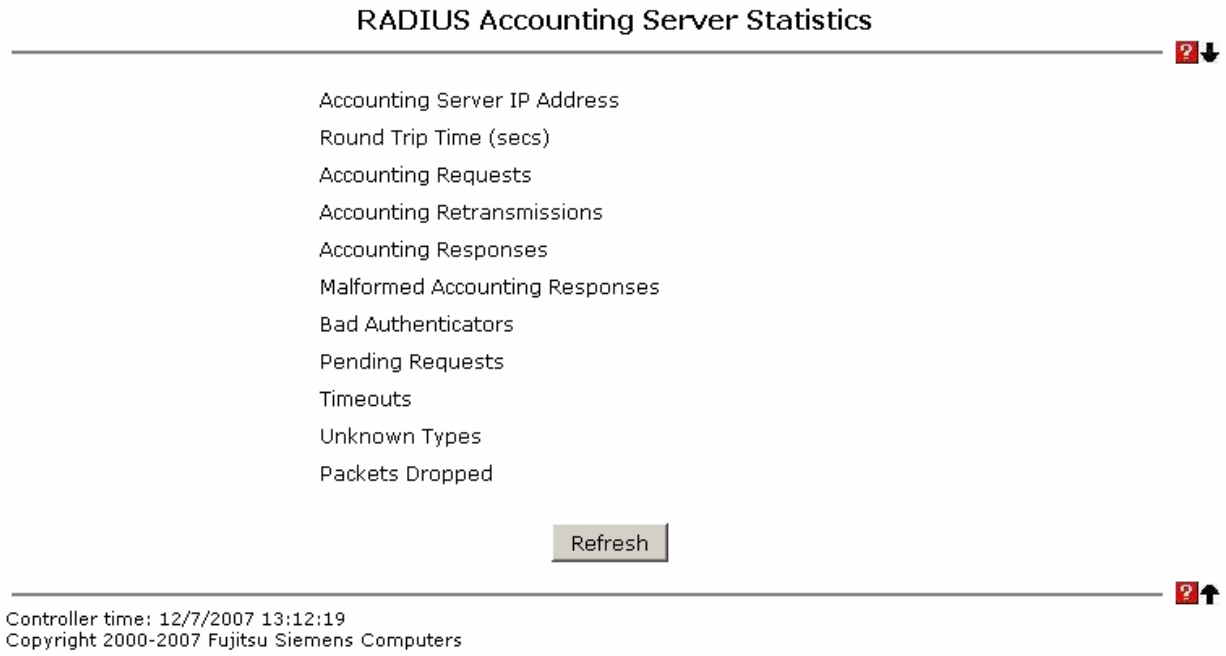
**Timeouts** - Displays the number of accounting timeouts to this server.

**Unknown Types** - Displays the number of RADIUS packets of unknown type that were received from this server on the accounting port.

**Packets Dropped** - Displays the number of RADIUS packets that were received from this server on the accounting port and dropped for some other reason.

**Command Buttons**

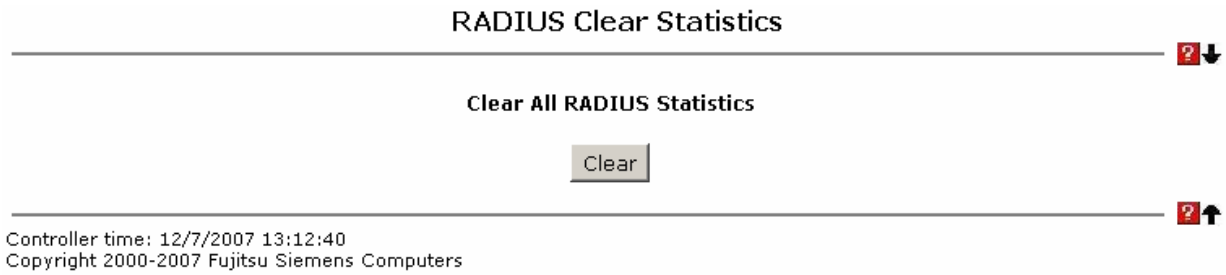
**Refresh** - Update the information on the page.




### 6.2.3.1.7 Resetting All RADIUS Statistics Page

**Command Buttons**

**Clear All RADIUS Statistics** - This button will clear the accounting server, authentication server, and RADIUS statistics.



### 6.2.3.2 Defining TACACS Configuration

#### 6.2.3.2.1 Configuring TACACS Configuration Page

Use this menu to configure the parameters for TACACS+, which is used to verify the login user's authentication. Note that only a user with Read/Write access privileges may change the data on this screen.

**Configurable Data**

**Authen. State** - TACACS+ administration mode which are Enable and Disable.

**Server ID** - The TACACS+ server index which are 1, 2, and 3.

**Authen. Server** - TACACS+ server IP address.

**Authen. Port** - The TCP port number of TACACS+.

**Server Time Out** - Timeout value of TACACS+ packet transmit.

**Retry Count** - Retry count after transmit timeout.

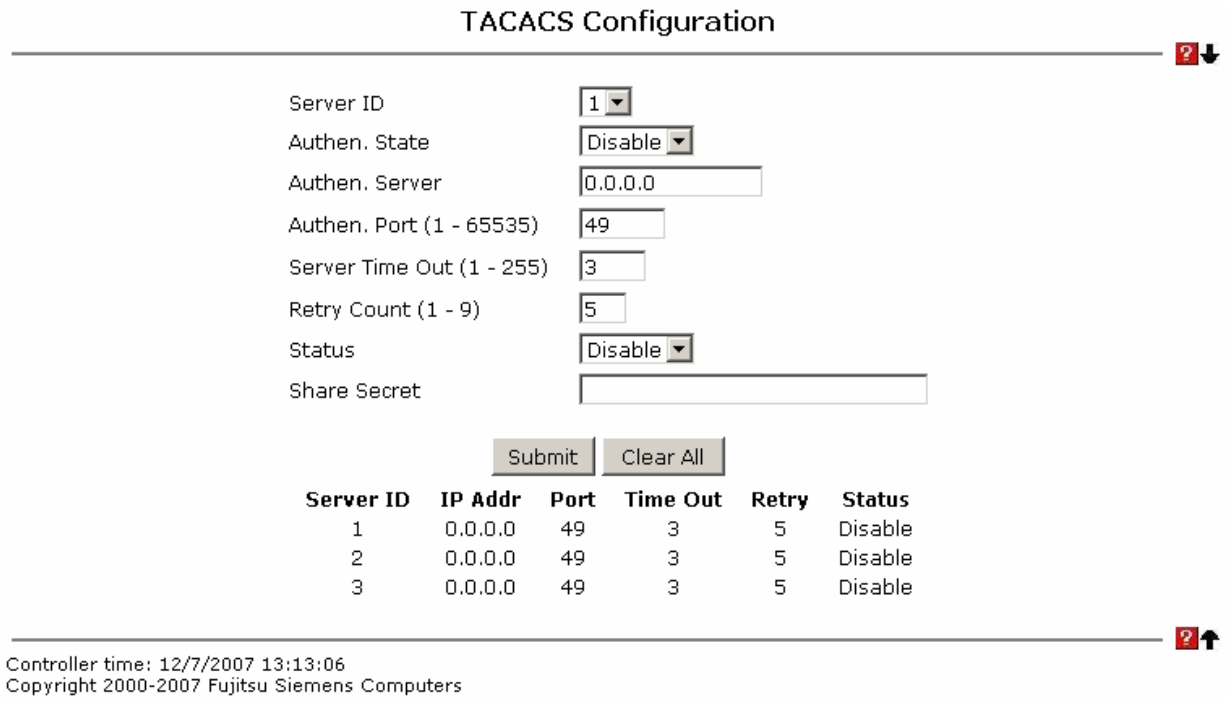
**Status** - The TACACS+ server status which are "disable", "master" and "slave".

**Share Secret** - The key only transmit between TACACS+ client and server..

**Command Buttons**

**Submit** - Send the updated screen to the IBP. Changes take effect on the IBP but these changes will not be retained across a power cycle unless a save is performed.

**Clear All** - Reset all configured to default.



### 6.2.3.3 Defining Secure HTTP Configuration

#### 6.2.3.3.1 Secure HTTP Configuration Page

**Configurable Data**

**Admin Mode** - This field is used to enable or disable the Administrative Mode of Secure HTTP. The currently configured value is shown when the web page is displayed. The default value is disabled.

**TLS Version 1** - This field is used to enable or disable Transport Layer Security Version 1.0. The currently configured value is shown when the web page is displayed. The default value is enabled.

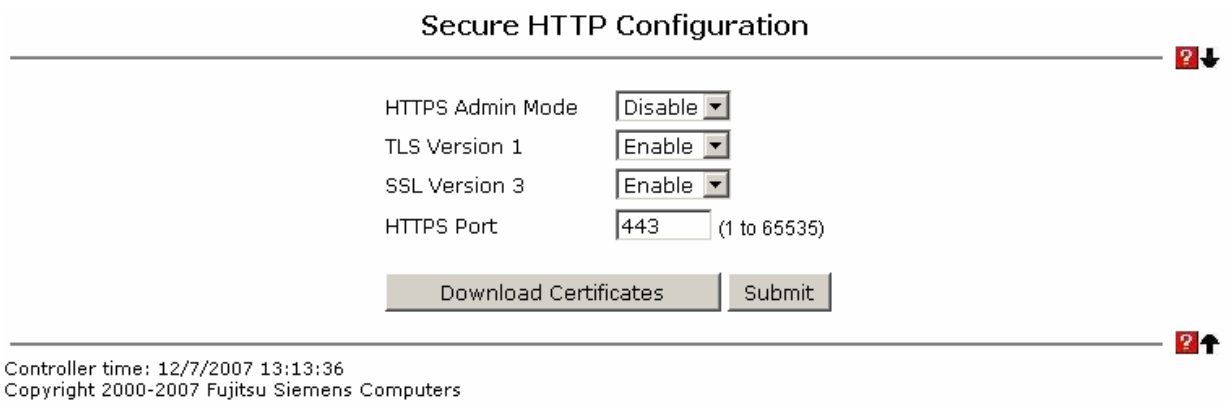
**SSL Version 3** - This field is used to enable or disable Secure Sockets Layer Version 3.0. The currently configured value is shown when the web page is displayed. The default value is enabled.

**HTTPS Port Number** - This field is used to set the HTTPS Port Number. The value must be in the range of 1 to 65535. Port 443 is the default value. The currently configured value is shown when the web page is displayed.

**Command Buttons**

**Submit** - Send the updated screen to the IBP. Changes take effect on the IBP but these changes will not be retained across a power cycle unless a save is performed.

**Download Certificates** - Link to the File Transfer page for the SSL Certificate download. Note that to download SSL Certificate files SSL must be administratively disabled.



#### 6.2.3.4 Defining Secure Shell Configuration

##### 6.2.3.4.1 Configuring Secure Shell Configuration Page

**Configurable Data**

**Admin Mode** - This select field is used to Enable or Disable the administrative mode of SSH. The currently configured value is shown when the web page is displayed. The default value is Disable.

**SSH Version 1** - This select field is used to Enable or Disable Protocol Level 1 for SSH. The currently configured value is shown when the web page is displayed. The default value is Enable.

**SSH Version 2** - This select field is used to Enable or Disable Protocol Level 2 for SSH. The currently configured value is shown when the web page is displayed. The default value is Enable.

**Maximum Number of SSH Sessions Allowed** - This select field is used to configure the maximum number of inbound SSH sessions allowed on the IBP. The currently configured value is shown when the web page is displayed. The range of acceptable values for this field is (0-5).

**SSH Session Timeout (Minutes)** - This text field is used to configure the inactivity timeout value for incoming SSH sessions to the IBP. The acceptable range for this value is (1-160) minutes.

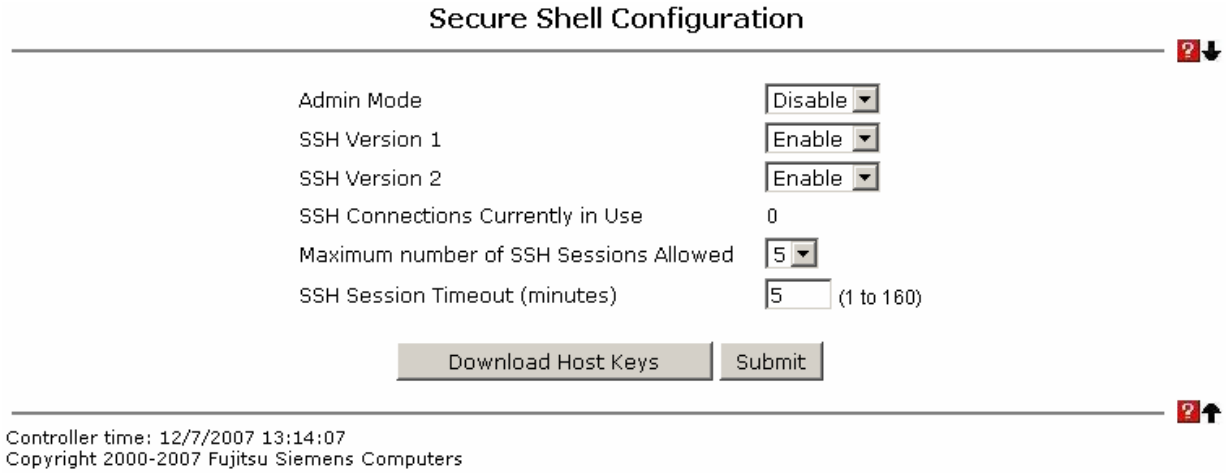
**Non-Configurable Data**

**SSH Connections in Use** - Displays the number of SSH connections currently in use in the system.

**Command Buttons**

**Submit** - Send the updated screen to the IBP. Changes take effect on the IBP but these changes will not be retained across a power cycle unless a save is performed.

**Download Host Keys** - Link to the File Transfer page for the Host Key download. Note that to download SSH key files SSH must be administratively disabled and there can be no active SSH sessions.


Secure Shell Configuration
Admin Mode
Disable
SSH Version 1
Enable
SSH Version 2
Enable
SSH Connections Currently in Use
0
Maximum number of SSH Sessions Allowed
5
SSH Session Timeout (minutes)
5
(1 to 160)
Download Host Keys
Submit
Controller time: 12/7/2007 13:14:07
Copyright 2000-2007 Fujitsu Siemens Computers

### 6.2.4 Extended Configuration Menu

#### 6.2.4.1 Viewing System Logs

##### 6.2.4.1.1 Viewing Buffered Log Configuration Page

This log stores messages in memory based upon the settings for message component and severity. On stackable systems, this log exists only on the top of stack platform. Other platforms in the stack forward their messages to the top of stack log.

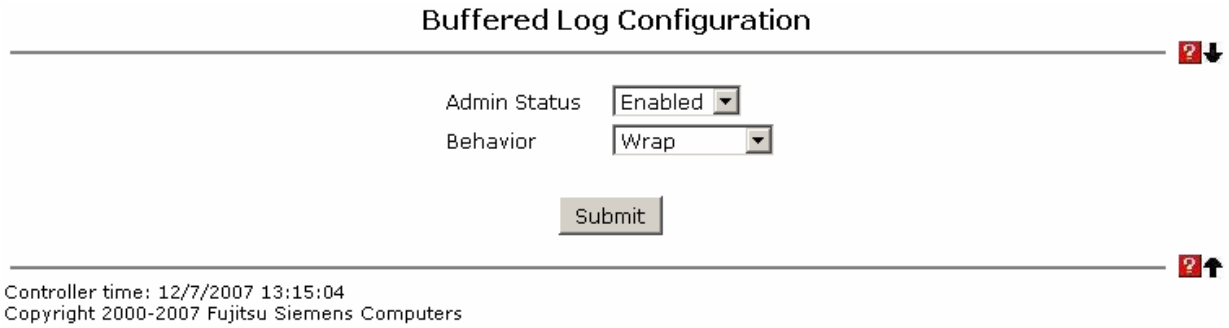
**Configurable Data**

**Admin Status** - A log that is "Disabled" shall not log messages. A log that is "Enabled" shall log messages. Enable or Disable logging by selecting the corresponding line on the pulldown entry field.

**Behavior** Indicates the behavior of the log when it is full. It can either wrap around or stop when the log space is filled.

**Command Buttons**

**Submit** - Update the IBP module with the values you entered.




##### 6.2.4.1.2 Viewing Buffered Log Page

This help message applies to the format of all logged messages which are displayed for the buffered log, persistent log, or console log.

**Format of the messages**

**<15>Aug 24 05:34:05 STK0 MSTP[2110]: mspt_api.c(318) 237 %% Interface 12 transitioned to root state on message age timer expiry**
-The above example indicates a user-level message (1) with severity 7 (debug) on a system that is not stack and generated by component MSTP running in thread id 2110 on

Aug 24 05:34:05 by line 318 of file mstp_api.c. This is the 237th message logged. Messages logged to a collector or relay via syslog have an identical format to the above message.

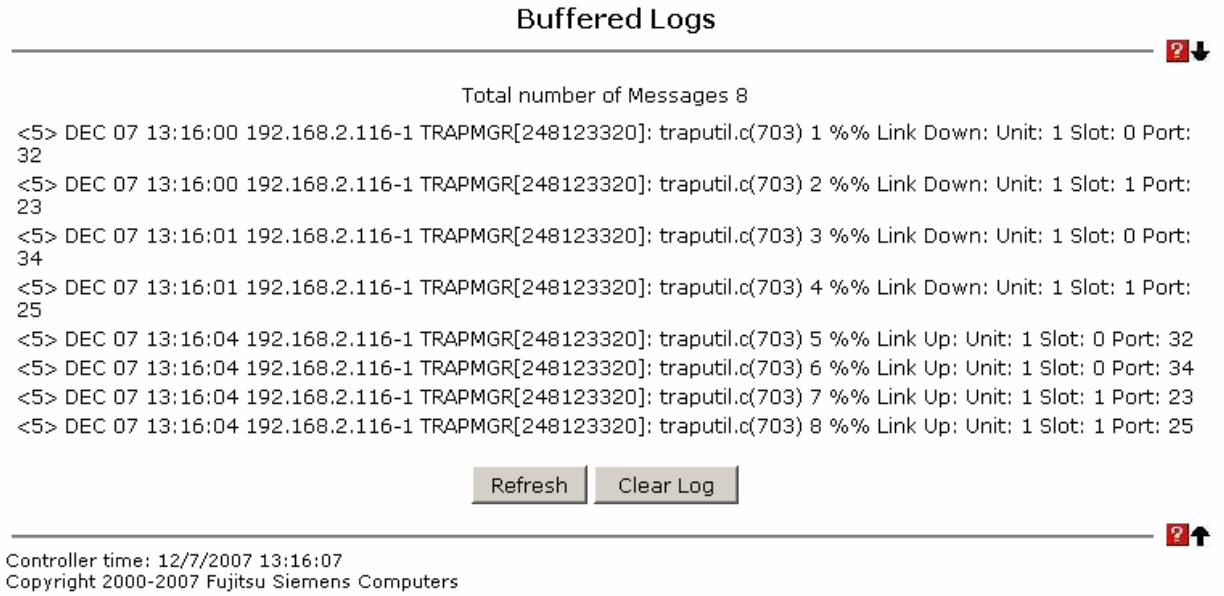
**Note for buffered log**

**Number of log messages displayed:** For the buffered log, only the latest 128 entries are displayed on the webpage

**Command Buttons**

**Refresh** - Refresh the page with the latest log entries.

**Clear Log** - Clear all entries in the log.


Buffered Logs
Total number of Messages 8
<5> DEC 07 13:16:00 192.168.2.116-1 TRAPMGR[248123320]: traputil.c(703) 1 %% Link Down: Unit: 1 Slot: 0 Port: 32
<5> DEC 07 13:16:00 192.168.2.116-1 TRAPMGR[248123320]: traputil.c(703) 2 %% Link Down: Unit: 1 Slot: 1 Port: 23
<5> DEC 07 13:16:01 192.168.2.116-1 TRAPMGR[248123320]: traputil.c(703) 3 %% Link Down: Unit: 1 Slot: 0 Port: 34
<5> DEC 07 13:16:01 192.168.2.116-1 TRAPMGR[248123320]: traputil.c(703) 4 %% Link Down: Unit: 1 Slot: 1 Port: 25
<5> DEC 07 13:16:04 192.168.2.116-1 TRAPMGR[248123320]: traputil.c(703) 5 %% Link Up: Unit: 1 Slot: 0 Port: 32
<5> DEC 07 13:16:04 192.168.2.116-1 TRAPMGR[248123320]: traputil.c(703) 6 %% Link Up: Unit: 1 Slot: 0 Port: 34
<5> DEC 07 13:16:04 192.168.2.116-1 TRAPMGR[248123320]: traputil.c(703) 7 %% Link Up: Unit: 1 Slot: 1 Port: 23
<5> DEC 07 13:16:04 192.168.2.116-1 TRAPMGR[248123320]: traputil.c(703) 8 %% Link Up: Unit: 1 Slot: 1 Port: 25
Refresh
Clear Log
Controller time: 12/7/2007 13:16:07
Copyright 2000-2007 Fujitsu Siemens Computers

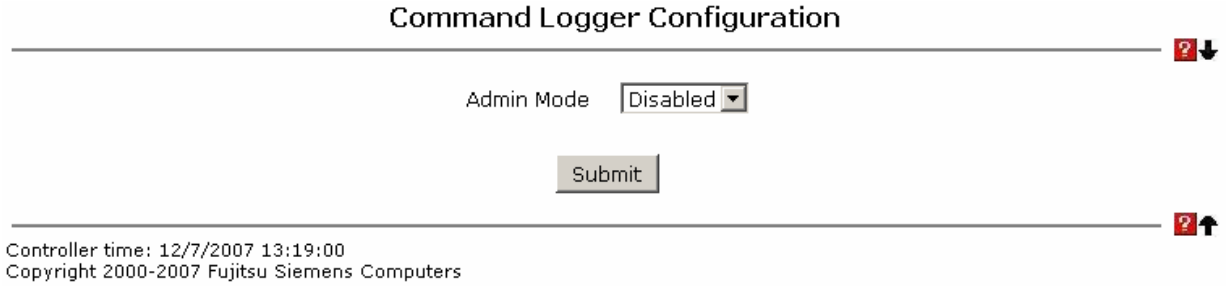
### 6.2.4.1.3 Configuring Command Logger Page

**Configurable Data**

**Admin Mode** - Enable/Disable the operation of the CLI Command logging by selecting the corresponding pulldown field and clicking Submit.

**Command Buttons**

**Submit** - Update the IBP module with the values you entered.




#### 6.2.4.1.4 Configuring Console Log Page

This allows logging to any serial device attached to the host.

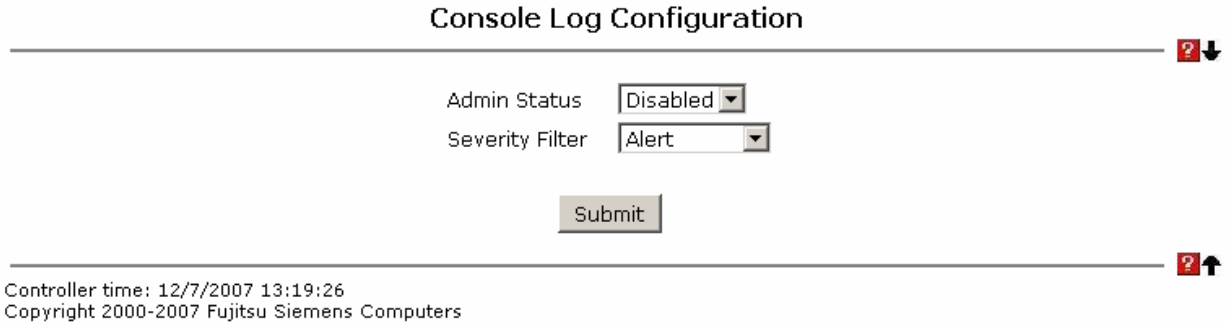
**Configurable Data**

**Admin Status** -A log that is "Disabled" shall not log messages. A log that is "Enabled" shall log messages. Enable or Disable logging by selecting the corresponding line on the pulldown entry field.

**Severity Filter** - A log records messages equal to or above a configured severity threshold. Select the severity option by selecting the corresponding line on the pulldown entry field. These severity levels have been enumerated below:
-Emergency (0): system is unusable
-Alert (1): action must be taken immediately
-Critical (2): critical conditions
-Error (3): error conditions
-Warning (4): warning conditions
-Notice(5): normal but significant conditions
-Informational(6): informational messages
-Debug(7): debug-level messages

**Command Buttons**

**Submit** - Update the IBP with the values you entered.




#### 6.2.4.1.5 Viewing Event Log Page

Use this panel to display the event log, which is used to hold error messages for catastrophic

events. After the event is logged and the updated log is saved in FLASH memory, the IBP module will be reset. The log can hold at least 2,000 entries (the actual number depends on the platform and OS), and the oldest one will be erased when an attempt is made to add an entry after it is full. The event log is preserved across system resets.

**Non-Configurable Data**

**Entry** - The number of the entry within the event log. The most recent entry is first.

**Filename** - The FASTPATH source code filename identifying the code that detected the event.

**Line** - The line number within the source file of the code that detected the event.

**Task ID** - The OS-assigned ID of the task reporting the event.

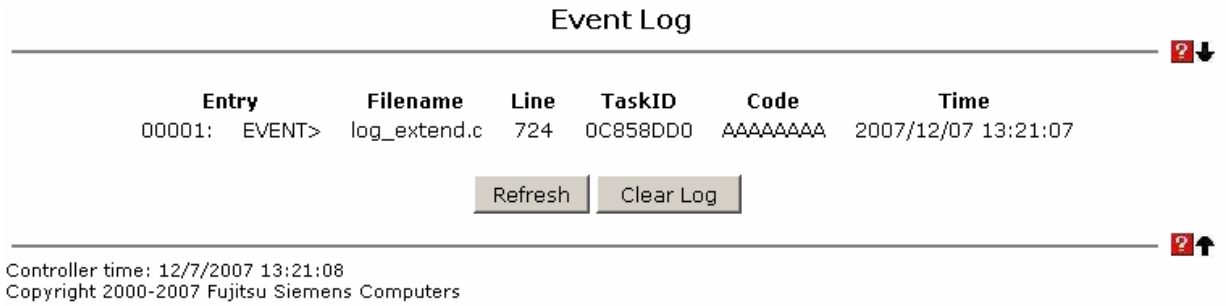
**Code** - The event code passed to the event log handler by the code reporting the event.

**Time** - The time the event occurred, measured from the previous reset.

**Command Buttons**

**Refresh** - Update the information on the page.

**Clear Log** - Remove all log information.




### 6.2.4.1.6 Configuring Hosts configuration Page

**Configurable Data**

**Host** - This is a list of the hosts that have been configured for syslog. Select a host for changing the configuration or choose to add a new hosts from the drop down list.

**IP Address** - This is the ip address of the host configured for syslog.

**Status** -This specifies wether the host has been configured to be actively logging or not. Set the host to be active/out of service from the drop down menu.

**Port** -This is the port on the host to which syslog messages are sent. The default port is 514. Specify the port in the text field.

**Severity Filter** -A log records messages equal to or above a configured severity threshold. Select the severity option by selecting the corresponding line on the pulldown entry field. These severity levels have been enumerated below:
-Emergency (0): system is unusable
-Alert (1): action must be taken immediately
-Critical (2): critical conditions

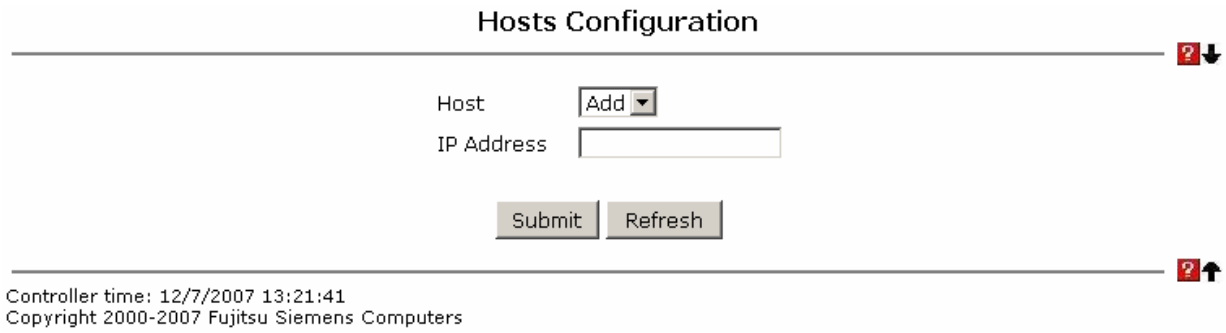
-Error (3): error conditions
-Warning (4): warning conditions
-Notice(5): normal but significant conditions
-Informational(6): informational messages
-Debug(7): debug-level messages

**Command Buttons**

**Submit** - Update the IBP with the values you entered.

**Refresh** - Refetch the database and display it again starting with the first entry in the table.

**Delete** - Delete a configured host.




#### 6.2.4.1.7 Configuring syslog configuration Page

**Configurable Data**

**Admin Status** -For enabling and disabling logging to configured syslog hosts. Setting this to disable stops logging to all syslog hosts. Disable means no messages will be sent to any collector/relay. Enable means messages will be sent to configured collector/relays using the values configured for each collector/relay. Enable/Disable the operation of the syslog function by selecting the corresponding line on the pulldown entry field.

**Local UDP Port** This is the port on the local host from which syslog messages are sent. The default port is 514. Specify the local port in the text field.

**Non-Configurable Data**

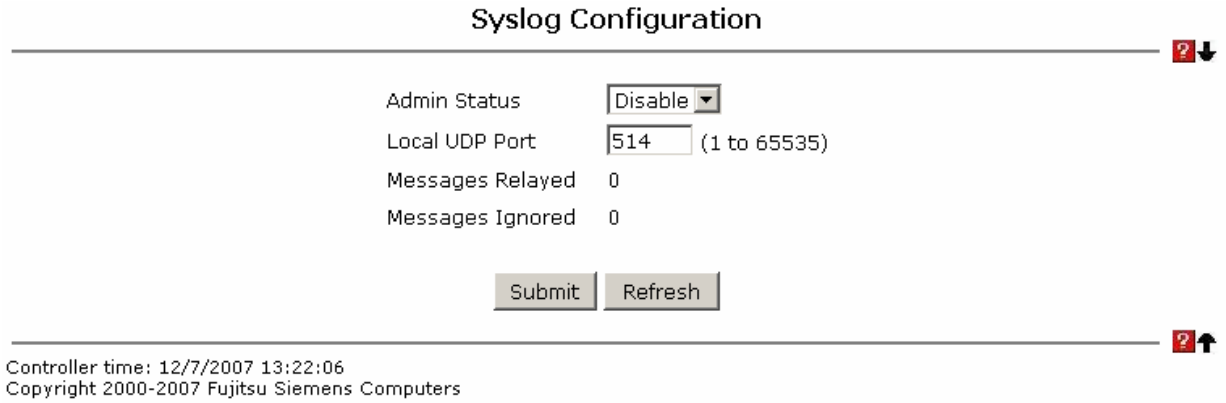
**Messages Relayed** - The count of syslog messages relayed.

**Messages Ignored** - The count of syslog messages ignored.

**Command Buttons**

**Submit** - Update the IBP module with the values you entered.

**Refresh** - Refetch the database and display it again starting with the first entry in the table.


Syslog Configuration
Admin Status
Disable
Local UDP Port
514
(1 to 65535)
Messages Relayed
0
Messages Ignored
0
Submit
Refresh
Controller time: 12/7/2007 13:22:06
Copyright 2000-2007 Fujitsu Siemens Computers

#### 6.2.4.1.8 Viewing Login Session Page

**Non-Configurable Data**

**ID** - Identifies the ID of this row.

**User Name** - Shows the user name of user who made the session.

**Connection From** - Shows the IP from which machine the user is connected.

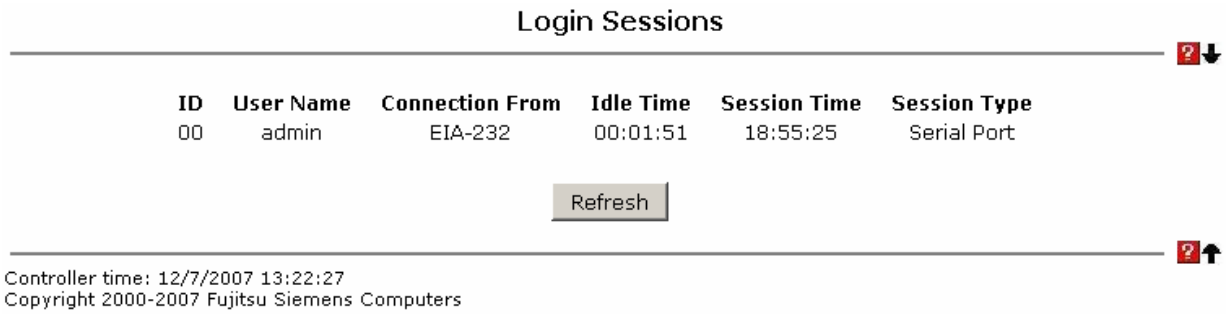
**Idle Time** - Shows the idle session time.

**Session Time** - Shows the total session time.

**Session Type** – Shows the type of session: telnet, serial or SSH.

**Command Buttons**

**Refresh** - Update the information on the page.



#### 6.2.4.2 Viewing Statistics

##### 6.2.4.2.1 Viewing the Panel Detailed Statistics Page

**Non-Configurable Data**

**ifIndex** - This object indicates the ifIndex of the interface table entry associated with the Processor of this IBP.

**Octets Received** - The total number of octets of data received by the processor (excluding framing bits but including FCS octets).

**Packets Received Without Errors** - The total number of packets (including broadcast packets and multicast packets) received by the processor.

**Unicast Packets Received** - The number of subnetwork-unicast packets delivered to a higher-layer protocol.

**Multicast Packets Received** - The total number of packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.

**Broadcast Packets Received** - The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.

**Receive Packets Discarded** - The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.

**Octets Transmitted** - The total number of octets transmitted out of the interface, including framing characters.

**Packets Transmitted Without Errors** - The total number of packets transmitted out of the interface.

**Unicast Packets Transmitted** - The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.

**Multicast Packets Transmitted** - The total number of packets that higher-level protocols requested be transmitted to a Multicast address, including those that were discarded or not sent.

**Broadcast Packets Transmitted** - The total number of packets that higher-level protocols requested be transmitted to the Broadcast address, including those that were discarded or not sent.

**Transmit Packets Discarded** - The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable

to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.

**Most Address Entries Ever Used** - The highest number of Forwarding Database Address Table entries that have been learned by this IBP since the most recent reboot.

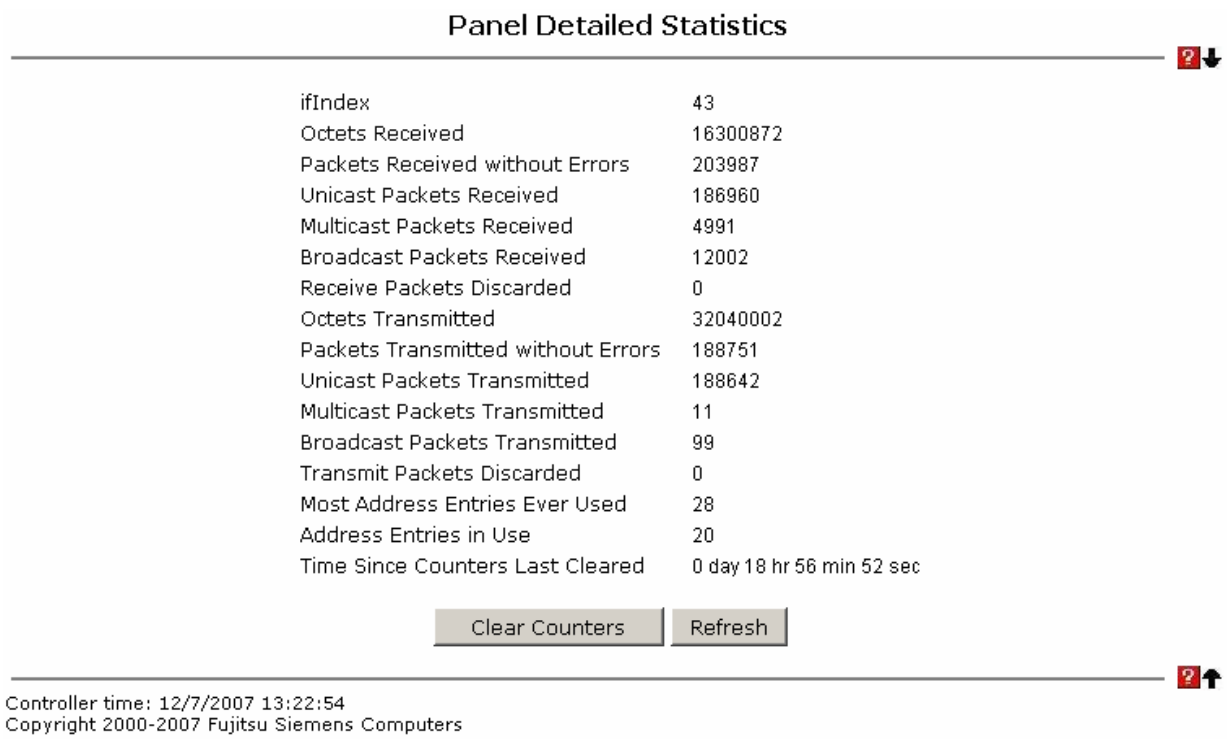
**Address Entries in Use** - The number of Learned and static entries in the Forwarding Database Address Table for this IBP.

**Time Since Counters Last Cleared** - The elapsed time, in days, hours, minutes, and seconds, since the statistics for this IBP were last cleared.

**Command Buttons**

**Clear Counters** - Clear all the counters, resetting all IBP summary and detailed statistics to default values. The discarded packets count cannot be cleared.

**Refresh** - Refresh the data on the screen with the present state of the data in the IBP.


Panel Detailed Statistics
ifIndex 43
Octets Received 16300872
Packets Received without Errors 203987
Unicast Packets Received 186960
Multicast Packets Received 4991
Broadcast Packets Received 12002
Receive Packets Discarded 0
Octets Transmitted 32040002
Packets Transmitted without Errors 188751
Unicast Packets Transmitted 188642
Multicast Packets Transmitted 11
Broadcast Packets Transmitted 99
Transmit Packets Discarded 0
Most Address Entries Ever Used 28
Address Entries in Use 20
Time Since Counters Last Cleared 0 day 18 hr 56 min 52 sec
Clear Counters
Refresh
Controller time: 12/7/2007 13:22:54
Copyright 2000-2007 Fujitsu Siemens Computers

### 6.2.4.2.2 Viewing the Panel Summary Statistics Page

**Non-Configurable Data**

**ifIndex** - This object indicates the ifIndex of the interface table entry associated with the Processor of this IBP.

**Packets Received Without Errors** - The total number of packets (including broadcast packets and multicast packets) received by the processor.

**Broadcast Packets Received** - The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.

**Packets Received with Errors** - The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.

**Packets Transmitted Without Errors** - The total number of packets transmitted out of the interface.

**Broadcast Packets Transmitted** - The total number of packets that higher-level protocols requested to be transmitted to the Broadcast address, including those that were discarded or not sent.

**Transmit Packet Errors** - The number of outbound packets that could not be transmitted because of errors.

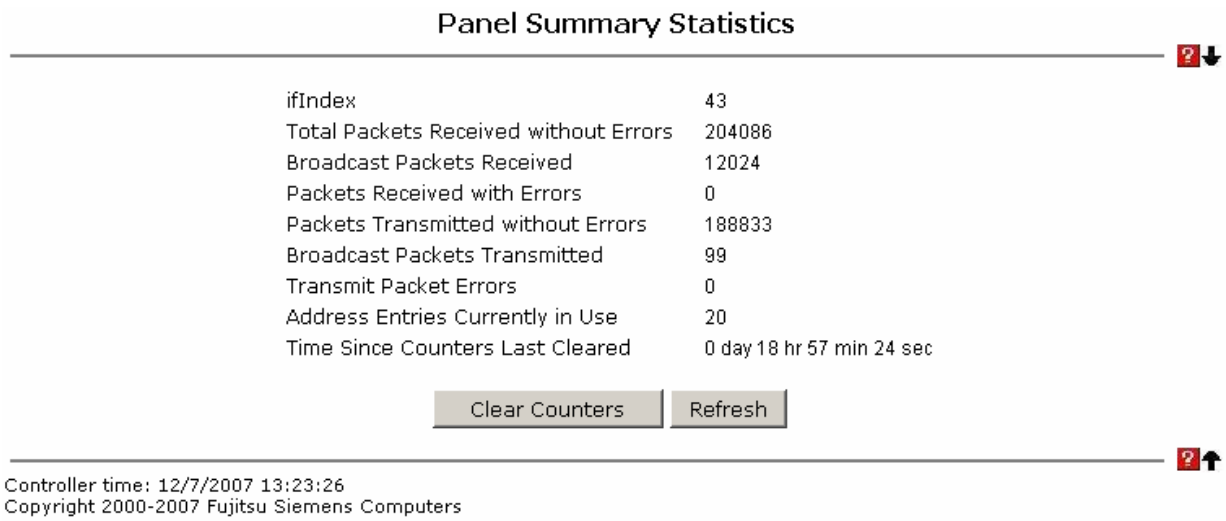
**Address Entries Currently in Use** - The total number of Forwarding Database Address Table entries now active on the IBP, including learned and static entries.

**Time Since Counters Last Cleared** - The elapsed time, in days, hours, minutes, and seconds since the statistics for this IBP were last cleared.

**Command Buttons**

**Clear Counters** - Clear all the counters, resetting all summary and detailed statistics to defaults. The discarded packets count cannot be cleared.

**Refresh** - Refresh the data on the screen with the present state of the data in the IBP.


Panel Summary Statistics
ifIndex 43
Total Packets Received without Errors 204086
Broadcast Packets Received 12024
Packets Received with Errors 0
Packets Transmitted without Errors 188833
Broadcast Packets Transmitted 99
Transmit Packet Errors 0
Address Entries Currently in Use 20
Time Since Counters Last Cleared 0 day 18 hr 57 min 24 sec
Clear Counters
Refresh
Controller time: 12/7/2007 13:23:26
Copyright 2000-2007 Fujitsu Siemens Computers

### 6.2.4.2.3 Viewing Each Port Detailed Statistics Page

**Selection Criteria**

**Slot/Port** - Selects the interface for which data is to be displayed or configured.

**Non-Configurable Data**

**ifIndex** - This object indicates the ifIndex of the interface table entry associated with this port on an adapter.

**Packets RX and TX 64 Octets** - The total number of packets (including bad packets) received or transmitted that were 64 octets in length (excluding framing bits but including FCS octets).

**Packets RX and TX 65-127 Octets** - The total number of packets (including bad packets) received or transmitted that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).

**Packets RX and TX 128-255 Octets** - The total number of packets (including bad packets) received or transmitted that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).

**Packets RX and TX 256-511 Octets** - The total number of packets (including bad packets) received or transmitted that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).

**Packets RX and TX 512-1023 Octets** - The total number of packets (including bad packets) received or transmitted that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).

**Packets RX and TX 1024-1518 Octets** - The total number of packets (including bad packets) received or transmitted that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).

**Packets RX and TX 1519-1522 Octets** - The total number of packets (including bad packets) received or transmitted that were between 1519 and 1522 octets in length inclusive (excluding framing bits but including FCS octets).

**Packets RX and TX 1523-2047 Octets** - The total number of packets (including bad packets) received or transmitted that were between 1523 and 2047 octets in length inclusive (excluding framing bits but including FCS octets).

**Packets RX and TX 2048-4095 Octets** - The total number of packets (including bad packets) received or transmitted that were between 2048 and 4095 octets in length inclusive (excluding framing bits but including FCS octets).

**Packets RX and TX 4096-9216 Octets** - The total number of packets (including bad packets) received or transmitted that were between 4096 and 9216 octets in length inclusive (excluding framing bits but including FCS octets).

**Octets Received** - The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets). This object can be used as a reasonable estimate of ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval.

**Packets Received 64 Octets** - The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).

**Packets Received 65-127 Octets** - The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).

**Packets Received 128-255 Octets** - The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).

**Packets Received 256-511 Octets** - The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).

**Packets Received 512-1023 Octets** - The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).

**Packets Received 1024-1518 Octets** - The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).

**Packets Received > 1522 Octets** - The total number of packets received that were longer than 1522 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.

**Total Packets Received Without Errors** - The total number of packets received that were without errors.

**Unicast Packets Received** - The number of subnetwork-unicast packets delivered to a higher-layer protocol.

**Multicast Packets Received** - The total number of good packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.

**Broadcast Packets Received** - The total number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets.

**Total Packets Received with MAC Errors** - The total number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.

**Jabbers Received** - The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). Note that this definition of jabber is different than the definition in IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). These documents define jabber as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms.

**Fragments Received** - The total number of packets received that were less than 64 octets in length with ERROR CRC(excluding framing bits but including FCS octets).

**Undersize Received** - The total number of packets received that were less than 64 octets in length with GOOD CRC(excluding framing bits but including FCS octets).

**Alignment Errors** - The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with a non-integral number of octets.

**Rx FCS Errors** - The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with an integral number of octets

**Overruns** - The total number of frames discarded as this port was overloaded with incoming packets, and could not keep up with the inflow.

**Total Packets Transmitted (Octets)** - The total number of octets of data (including those in bad packets) transmitted on the network (excluding framing bits but including FCS octets). This object can be used as a reasonable estimate of ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval.

**Packets Transmitted 64 Octets** - The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).

**Packets Transmitted 65-127 Octets** - The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).

**Packets Transmitted 128-255 Octets** - The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).

**Packets Transmitted 256-511 Octets** - The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).

**Packets Transmitted 512-1023 Octets** - The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).

**Packets Transmitted 1024-1518 Octets** - The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).

**Packets Transmitted 1523-2047 Octets** - The total number of packets (including bad packets) received that were between 1523 and 2047 octets in length inclusive (excluding framing bits but including FCS octets).

**Packets Transmitted 2048-4095 Octets** - The total number of packets (including bad packets) received that were between 2048 and 4095 octets in length inclusive (excluding framing bits but including FCS octets).

**Packets Transmitted 4096-9216 Octets** - The total number of packets (including bad packets) received that were between 4096 and 9216 octets in length inclusive (excluding framing bits but including FCS octets).

**Maximum Frame Size** - The maximum ethernet frame size the interface supports or is configured, including ethernet header, CRC, and payload. (1518 to 9216). The default maximum frame size is 1518 .

**Total Packets Transmitted Successfully** - The number of frames that have been transmitted by this port to its segment.

**Unicast Packets Transmitted** - The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.

**Multicast Packets Transmitted** - The total number of packets that higher-level protocols requested be transmitted to a Multicast address, including those that were discarded or not sent.

**Broadcast Packets Transmitted** - The total number of packets that higher-level protocols requested be transmitted to the Broadcast address, including those that were discarded or not sent.

**Total Transmit Errors** - The sum of Single, Multiple, and Excessive Collisions.

**Tx FCS Errors** - The total number of packets transmitted that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with an integral number of octets

**Tx Oversized** - The total nummber of frames that exceeded the max permitted frame size. This counter has a max increment rate of 815 counts per sec at 10 Mb/s.

**Underrun Errors** - The total number of frames discarded because the transmit FIFO buffer became empty during frame transmission.

**Total Transmit Packets Discarded** - The sum of single collision frames discarded, multiple collision frames discarded, and excessive frames discarded.

**Single Collision Frames** - A count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision.

**Multiple Collision Frames** - A count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision.

**Excessive Collision Frames** - A count of frames for which transmission on a particular interface fails due to excessive collisions.

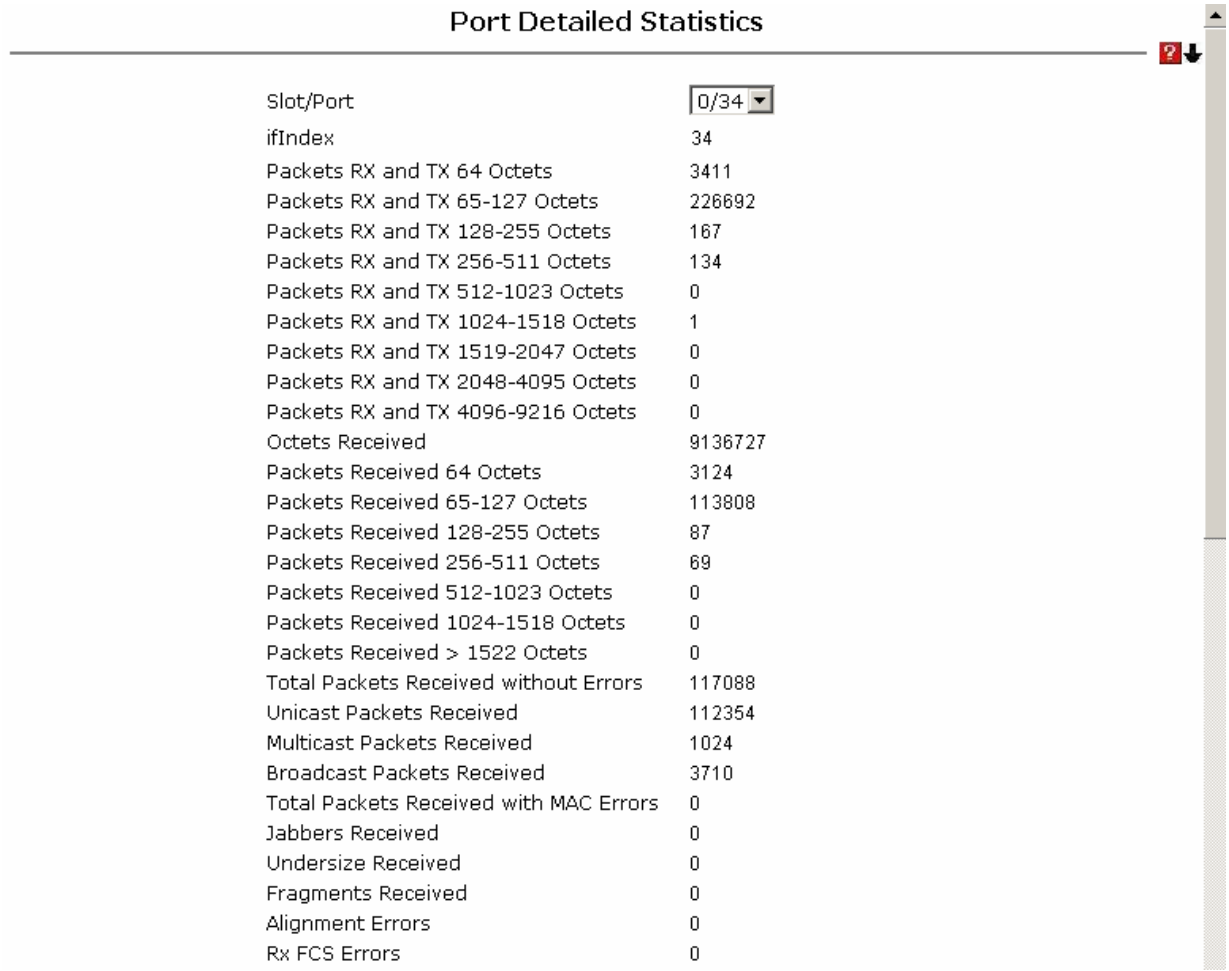
**Time Since Counters Last Cleared** - The elapsed time, in days, hours, minutes, and seconds since the statistics for this port were last cleared.

**Command Buttons**

**Clear Counters** - Clear all the counters, resetting all statistics for this port to default values.

**Clear All Counters** - Clear all the counters for all ports, resetting all statistics for all ports to default values.

**Refresh** - Refresh the data on the screen with the present state of the data in the IBP.



Port Detailed Statistics

| | |
|---|---|
| Slot/Port | 0/34 |
| ifIndex | 34 |
| Packets RX and TX 64 Octets | 3411 |
| Packets RX and TX 65-127 Octets | 226692 |
| Packets RX and TX 128-255 Octets | 167 |
| Packets RX and TX 256-511 Octets | 134 |
| Packets RX and TX 512-1023 Octets | 0 |
| Packets RX and TX 1024-1518 Octets | 1 |
| Packets RX and TX 1519-2047 Octets | 0 |
| Packets RX and TX 2048-4095 Octets | 0 |
| Packets RX and TX 4096-9216 Octets | 0 |
| Octets Received | 9136727 |
| Packets Received 64 Octets | 3124 |
| Packets Received 65-127 Octets | 113808 |
| Packets Received 128-255 Octets | 87 |
| Packets Received 256-511 Octets | 69 |
| Packets Received 512-1023 Octets | 0 |
| Packets Received 1024-1518 Octets | 0 |
| Packets Received > 1522 Octets | 0 |
| Total Packets Received without Errors | 117088 |
| Unicast Packets Received | 112354 |
| Multicast Packets Received | 1024 |
| Broadcast Packets Received | 3710 |
| Total Packets Received with MAC Errors | 0 |
| Jabbers Received | 0 |
| Undersize Received | 0 |
| Fragments Received | 0 |
| Alignment Errors | 0 |
| Rx FCS Errors | 0 |

| | |
|---|---|
| Overruns | 0 |
| Receive Packets Discarded | 184 |
| Total Packets Transmitted (Octets) | 8872657 |
| Packets Transmitted 64 Octets | 287 |
| Packets Transmitted 65-127 Octets | 112884 |
| Packets Transmitted 128-255 Octets | 80 |
| Packets Transmitted 256-511 Octets | 65 |
| Packets Transmitted 512-1023 Octets | 0 |
| Packets Transmitted 1024-1518 Octets | 1 |
| Total Packets Transmitted Successfully | 113317 |
| Unicast Packets Transmitted | 111984 |
| Multicast Packets Transmitted | 936 |
| Broadcast Packets Transmitted | 397 |
| Tx Oversized | 0 |
| Total Transmit Errors | 0 |
| Tx FCS Errors | 0 |
| Underrun Errors | 0 |
| Total Transmit Packets Discarded | 0 |
| Single Collision Frames | 0 |
| Multiple Collision Frames | 0 |
| Excessive Collision Frames | 0 |
| Packets Dropped by MMU | 0 |
| Time Since Counters Last Cleared | 0 day 18 hr 58 min 2 sec |

#### 6.2.4.2.4 Viewing Each Port Summary Statistics Page

**Selection Criteria**

**Slot/Port** - Selects the interface for which data is to be displayed or configured.

**Non-Configurable Data**

**ifIndex** - This object indicates the ifIndex of the interface table entry associated with this port on an adapter.

**Total Packets Received without Errors** - The total number of packets received that were without errors.

**Packets Received with Errors** - The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.

**Broadcast Packets Received** - The total number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets.

**Packets Transmitted without Errors** - The number of frames that have been transmitted by this port to its segment.

**Transmit Packet Errors** - The number of outbound packets that could not be transmitted because of errors.

**Collision Frames** - The best estimate of the total number of collisions on this Ethernet segment.

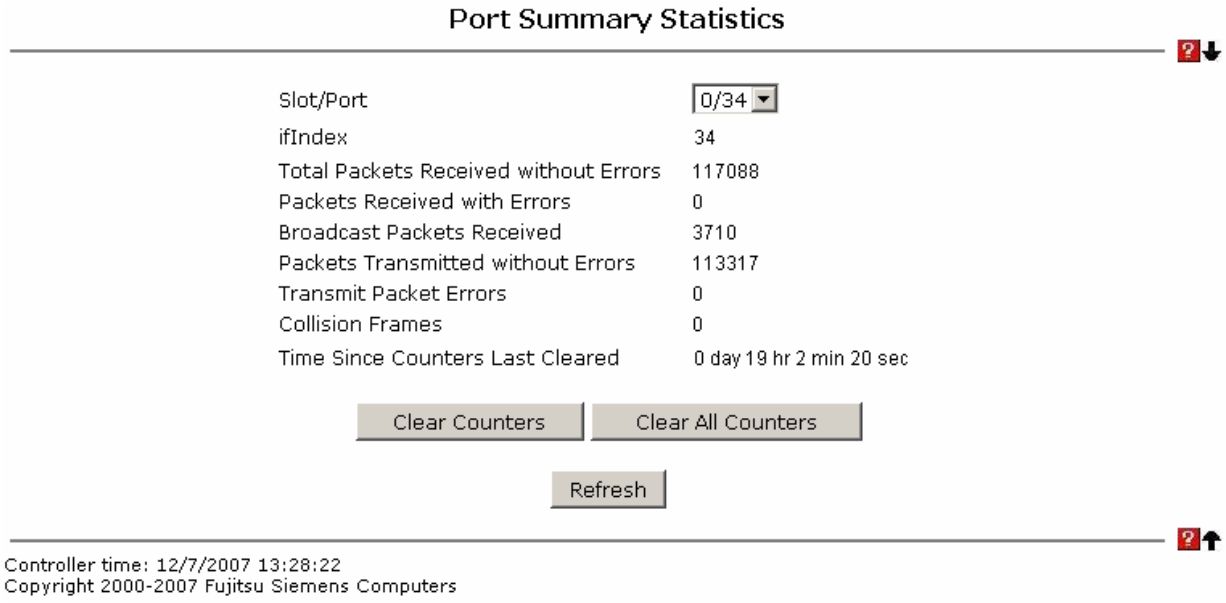
**Time Since Counters Last Cleared** - The elapsed time, in days, hours, minutes, and seconds since the statistics for this port were last cleared.

**Command Buttons**

**Clear Counters** - Clears all the counters, resetting all statistics for this port to default values.

**Clear All Counters** - Clears all the counters for all ports, resetting all statistics for all ports to default values.

**Refresh** – Refreshes the data on the screen with the present state of the data in the IBP.



### 6.2.4.3 Managing Access Control (802.1x)

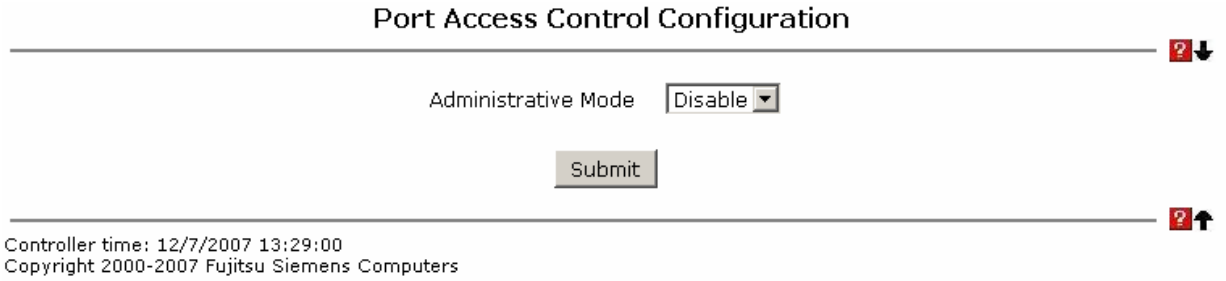
#### 6.2.4.3.1 Defining Access Control Page

**Configurable Data**

**Administrative Mode** - This selector lists the two options for administrative mode: enable and disable. The default value is disabled.

**Command Buttons**

**Submit** - Sends the updated screen to the IBP and causes the changes to take effect on the IBP but these changes will not be retained across a power cycle unless a save is performed.




#### 6.2.4.3.2 Configuring each Port Access Control Configuration Page

**Selection Criteria**

**Port** - Selects the port to be configured. When the selection is changed, a screen refresh will occur causing all fields to be updated for the newly selected port. All physical interfaces are valid.

**Configurable Data**

**Control Mode** - This selector lists the options for control mode. The control mode is only set if the link status of the port is link up. The options are:

*force unauthorized:* The authenticator port access entity (PAE) unconditionally sets the controlled port to unauthorized

*force authorized:* The authenticator PAE unconditionally sets the controlled port to authorized.

*auto:* The authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator, and the authentication server.

**Quiet Period** - This input field allows the user to configure the quiet period for the selected port. This command sets the value, in seconds, of the timer used by the authenticator state machine on this port to define periods of time in which it will not attempt to acquire a supplicant. The quiet period is the period for which the authenticator does not attempt to acquire a supplicant after a failed authentication exchange with the supplicant. The quiet period must be a number in the range of 0 and 65535. A quiet period value of 0 means that the authenticator state machine will never acquire a supplicant. The default value is 60. Changing the value will not change the configuration until the Submit button is pressed.

**Transmit Period** - This input field allows the user to configure the transmit period for the selected port. The transmit period is the value, in seconds, of the timer used by the authenticator state machine on the specified port to determine when to send an EAPOL

EAP Request/Identity frame to the supplicant. The transmit period must be a number in the range of 1 to 65535. The default value is 30. Changing the value will not change the configuration until the Submit button is pressed.

**Supplicant Timeout** - This input field allows the user to enter the supplicant timeout for the selected port. The supplicant timeout is the value, in seconds, of the timer used by the authenticator state machine on this port to timeout the supplicant. The supplicant timeout must be a value in the range of 1 to 65535. The default value is 30. Changing the value will not change the configuration until the Submit button is pressed.

**Server Timeout** - This input field allows the user to enter the server timeout for the selected port. The server timeout is the value, in seconds, of the timer used by the authenticator on this port to timeout the authentication server. The server timeout must be a value in the range of 1 to 65535. The default value is 30. Changing the value will not change the configuration until the Submit button is pressed.

**Maximum Requests** - This input field allows the user to enter the maximum requests for the selected port. The maximum requests value is the maximum number of times the authenticator state machine on this port will retransmit an EAPOL EAP Request/Identity before timing out the supplicant. The maximum requests value must be in the range of 1 to 10. The default value is 2. Changing the value will not change the configuration until the Submit button is pressed.

**Reauthentication Period** - This input field allows the user to enter the reauthentication period for the selected port. The reauthentication period is the value, in seconds, of the timer used by the authenticator state machine on this port to determine when reauthentication of the supplicant takes place. The reauthentication period must be a value in the range of 1 to 65535. The default value is 3600. Changing the value will not change the configuration until the Submit button is pressed.

**Reauthentication Enabled** - This field allows the user to enable or disable reauthentication of the supplicant for the specified port. The selectable values are 'true' and 'false'. If the value is 'true' reauthentication will occur. Otherwise, reauthentication will not be allowed. The default value is false. Changing the selection will not change the configuration until the Submit button is pressed.

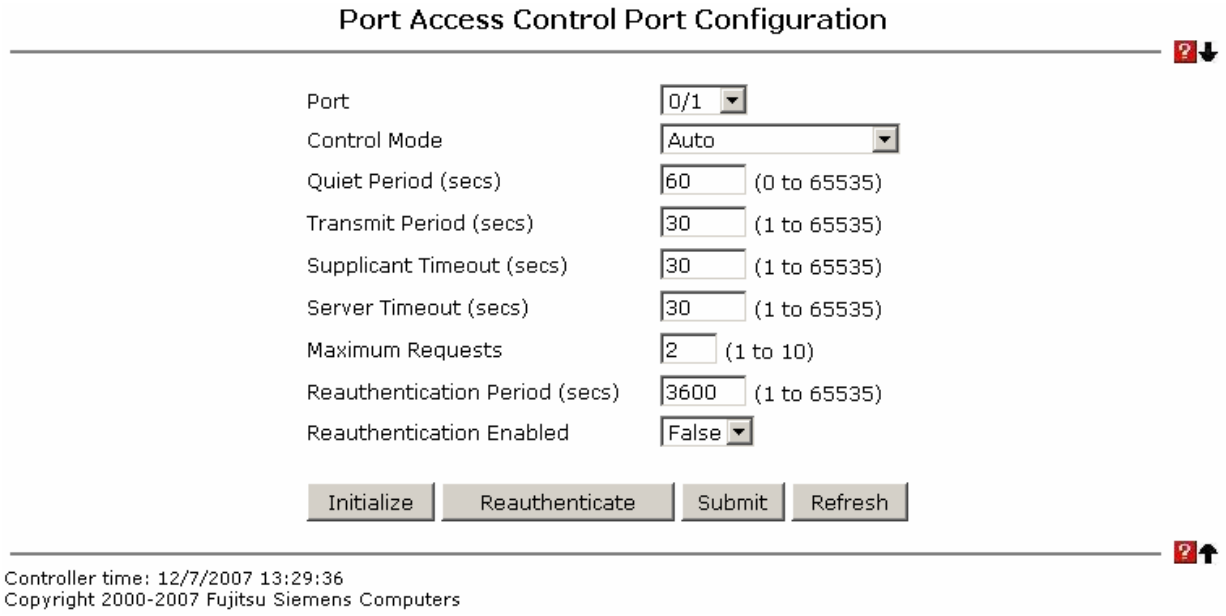
**Command Buttons**

**Initialize** - This button begins the initialization sequence on the selected port. This button is only selectable if the control mode is 'auto'. If the button is not selectable, it will be grayed out. Once this button is pressed, the action is immediate. It is not required to press the Submit button for the action to occur.

**Reauthenticate** - This button begins the reauthentication sequence on the selected port. This button is only selectable if the control mode is 'auto'. If the button is not selectable, it will be grayed out. Once this button is pressed, the action is immediate. It is not required to press the Submit button for the action to occur.

**Submit** - Sends the updated screen to the IBP and causes the changes to take effect on the IBP but these changes will not be retained across a power cycle unless a save is performed.

**Refresh** - Update the information on the page.




#### 6.2.4.3.3 Viewing each Port Access Control Configuration Information Page

**Selection Criteria**

**Port** - Selects the port to be displayed. When the selection is changed, a screen refresh will occur causing all fields to be updated for the newly selected port. All physical interfaces are valid.

**Non-Configurable Data**

**Control Mode** - Displays the configured control mode for the specified port. Options are:

*force unauthorized:* The authenticator port access entity (PAE) unconditionally sets the controlled port to unauthorized

*force authorized:* The authenticator PAE unconditionally sets the controlled port to authorized.

*auto:* The authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator, and the authentication server.

**Quiet Period** - This field displays the configured quiet period for the selected port. This quiet period is the value, in seconds, of the timer used by the authenticator state machine on this port to define periods of time in which it will not attempt to acquire a supplicant. The quiet period is the period for which the authenticator does not attempt to acquire a supplicant after a failed authentication exchange with the supplicant. The quiet period is a number in the range of 0 and 65535.

**Transmit Period** - This field displays the configured transmit period for the selected port. The transmit period is the value, in seconds, of the timer used by the authenticator state machine on the specified port to determine when to send an EAPOL EAP Request/Identity frame to the supplicant. The transmit period is a number in the range of 1 to 65535.

**Supplicant Timeout** - This field displays the configured supplicant timeout for the selected port. The supplicant timeout is the value, in seconds, of the timer used by the authenticator state machine on this port to timeout the supplicant. The supplicant timeout is a value in the range of 1 to 65535.

**Server Timeout** - This field displays the configured server timeout for the selected port. The server timeout is the value, in seconds, of the timer used by the authenticator on this port to timeout the authentication server. The server timeout is a value in the range of 1 to 65535.

**Maximum Requests** - This field displays the configured maximum requests for the selected port. The maximum requests value is the maximum number of times the authenticator state machine on this port will retransmit an EAPOL EAP Request/Identity before timing out the supplicant. The maximum requests value is in the range of 1 to 10.

**Reauthentication Period** - This field displays the configured reauthentication period for the selected port. The reauthentication period is the value, in seconds, of the timer used by the authenticator state machine on this port to determine when reauthentication of the supplicant takes place. The reauthentication period is a value in the range of 1 to 65535.

**Reauthentication Enabled** - This field displays if reauthentication is enabled on the selected port. This is a configurable field. The possible values are 'true' and 'false'. If the value is 'true' reauthentication will occur. Otherwise, reauthentication will not be allowed.

**Control Direction** - This displays the control direction for the specified port. The control direction dictates the degree to which protocol exchanges take place between Supplicant and Authenticator. This affects whether the unauthorized controlled port exerts control over communication in both directions (disabling both incoming and outgoing frames) or just in the incoming direction (disabling only the reception of incoming frames). This field is not configurable on some platforms.

**Protocol Version** - This field displays the protocol version associated with the selected port. The only possible value is 1, corresponding to the first version of the 802.1x specification. This field is not configurable.

**PAE Capabilities** - This field displays the port access entity (PAE) functionality of the selected port. Possible values are "Authenticator" or "Supplicant". This field is not configurable.

**Authenticator PAE State** - This field displays the current state of the authenticator PAE state machine. Possible values are:

"Initialize"

"Disconnected"

"Connecting"

"Authenticating"

"Authenticated"

"Aborting"

"Held"

"ForceAuthorized"

"ForceUnauthorized".

**Backend State** - This field displays the current state of the backend authentication state machine. Possible values are:

"Request"

"Response"

"Success"

"Fail"

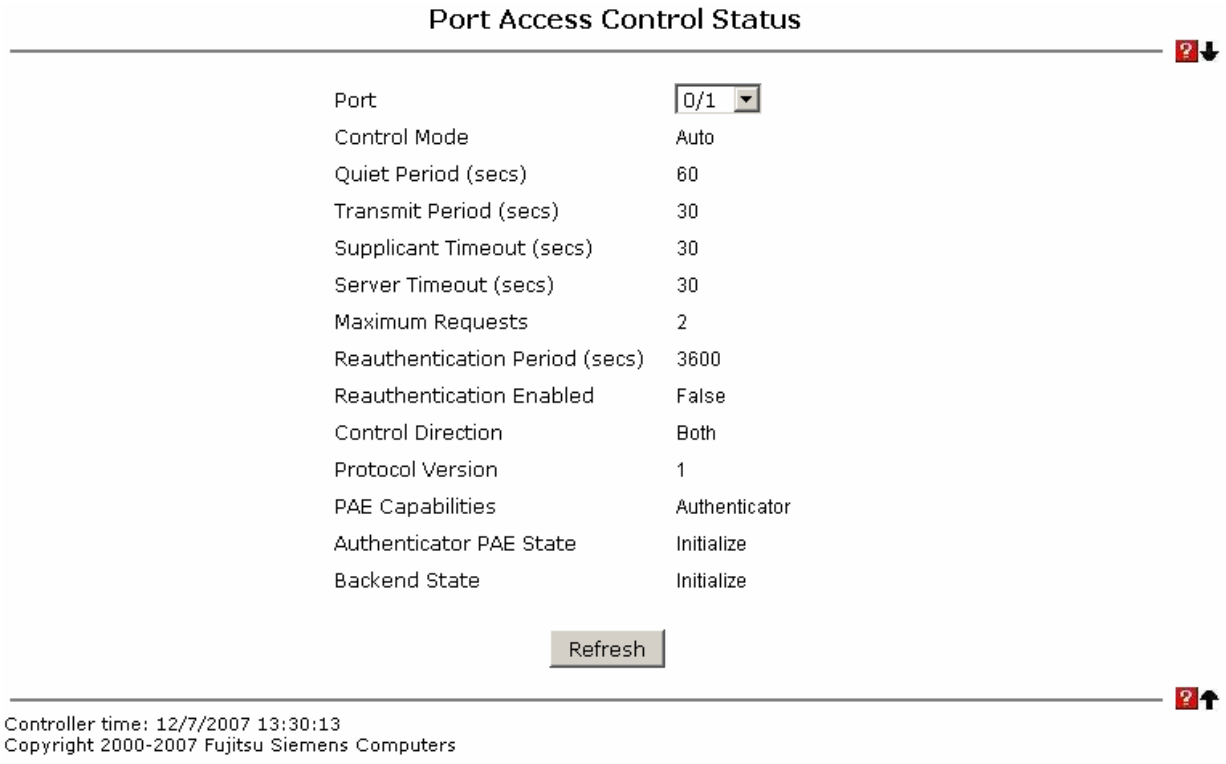
"Timeout"

"Initialize"

"Idle"

**Command Buttons**

**Refresh** - Update the information on the page.




### 6.2.4.3.4 Viewing Access Control Summary Page

**Non-Configurable Data**

**Port** - Specifies the port whose settings are displayed in the current table row.

**Control Mode** - This field indicates the configured control mode for the port. Possible values are:

*Force Unauthorized:* The authenticator port access entity (PAE) unconditionally sets the controlled port to unauthorized.

*Force Authorized:* The authenticator PAE unconditionally sets the controlled port to authorized.

*Auto:* The authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator, and the authentication server.

**Operating Control Mode** - This field indicates the control mode under which the port is actually operating. Possible values are:

ForceUnauthorized

ForceAuthorized

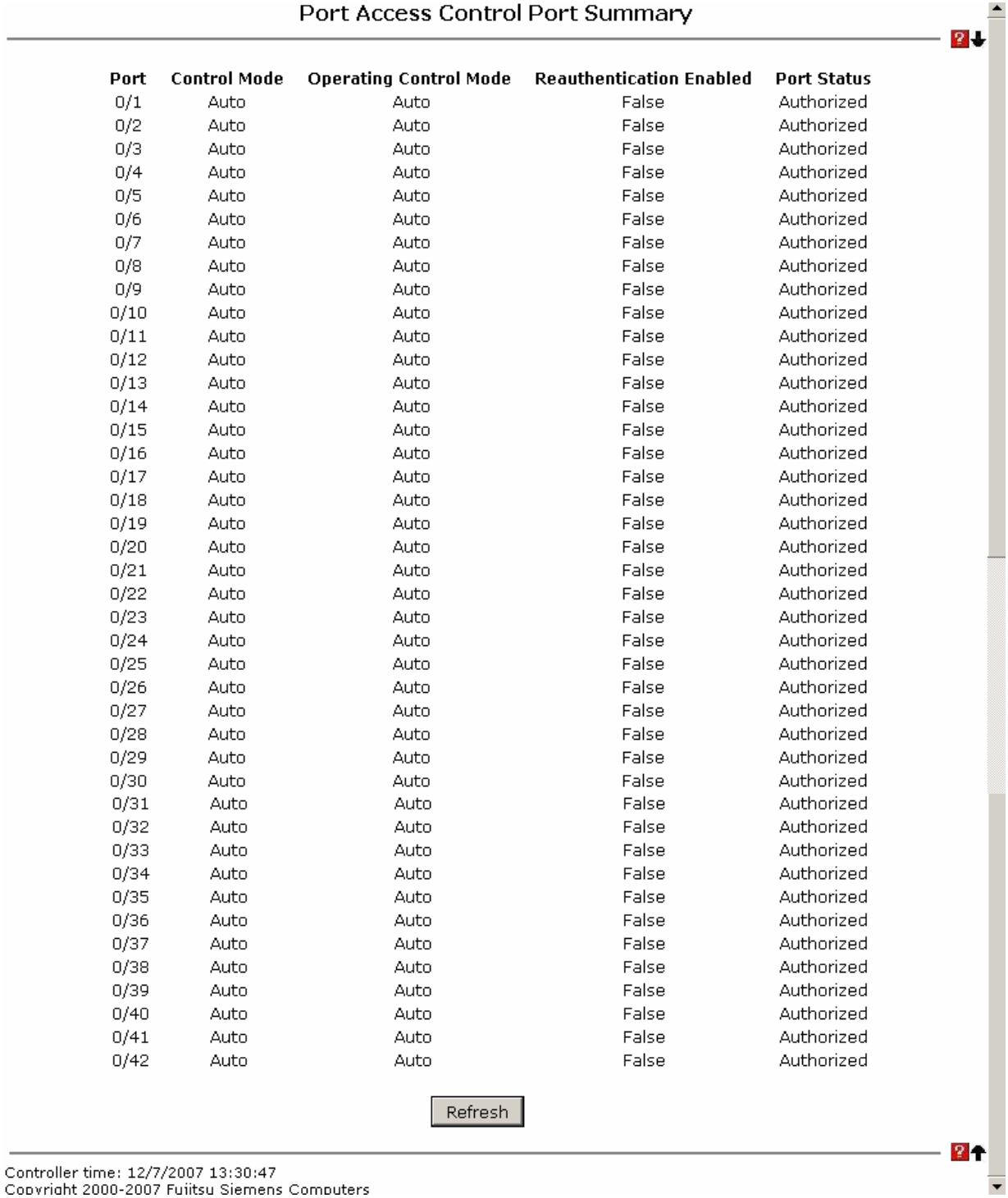
Auto

**Reauthentication Enabled** - This field shows whether reauthentication of the supplicant for the specified port is allowed. The possible values are 'true' and 'false'. If the value is 'true' reauthentication will occur. Otherwise, reauthentication will not be allowed.

**Port Status** - This field shows the authorization status of the specified port. The possible values are 'Authorized' and 'Unauthorized'.

### Command Buttons

**Refresh** - Update the information on the page.



Port Access Control Port Summary

| Port | Control Mode | Operating Control Mode | Reauthentication Enabled | Port Status |
|---|---|---|---|---|
| 0/1 | Auto | Auto | False | Authorized |
| 0/2 | Auto | Auto | False | Authorized |
| 0/3 | Auto | Auto | False | Authorized |
| 0/4 | Auto | Auto | False | Authorized |
| 0/5 | Auto | Auto | False | Authorized |
| 0/6 | Auto | Auto | False | Authorized |
| 0/7 | Auto | Auto | False | Authorized |
| 0/8 | Auto | Auto | False | Authorized |
| 0/9 | Auto | Auto | False | Authorized |
| 0/10 | Auto | Auto | False | Authorized |
| 0/11 | Auto | Auto | False | Authorized |
| 0/12 | Auto | Auto | False | Authorized |
| 0/13 | Auto | Auto | False | Authorized |
| 0/14 | Auto | Auto | False | Authorized |
| 0/15 | Auto | Auto | False | Authorized |
| 0/16 | Auto | Auto | False | Authorized |
| 0/17 | Auto | Auto | False | Authorized |
| 0/18 | Auto | Auto | False | Authorized |
| 0/19 | Auto | Auto | False | Authorized |
| 0/20 | Auto | Auto | False | Authorized |
| 0/21 | Auto | Auto | False | Authorized |
| 0/22 | Auto | Auto | False | Authorized |
| 0/23 | Auto | Auto | False | Authorized |
| 0/24 | Auto | Auto | False | Authorized |
| 0/25 | Auto | Auto | False | Authorized |
| 0/26 | Auto | Auto | False | Authorized |
| 0/27 | Auto | Auto | False | Authorized |
| 0/28 | Auto | Auto | False | Authorized |
| 0/29 | Auto | Auto | False | Authorized |
| 0/30 | Auto | Auto | False | Authorized |
| 0/31 | Auto | Auto | False | Authorized |
| 0/32 | Auto | Auto | False | Authorized |
| 0/33 | Auto | Auto | False | Authorized |
| 0/34 | Auto | Auto | False | Authorized |
| 0/35 | Auto | Auto | False | Authorized |
| 0/36 | Auto | Auto | False | Authorized |
| 0/37 | Auto | Auto | False | Authorized |
| 0/38 | Auto | Auto | False | Authorized |
| 0/39 | Auto | Auto | False | Authorized |
| 0/40 | Auto | Auto | False | Authorized |
| 0/41 | Auto | Auto | False | Authorized |
| 0/42 | Auto | Auto | False | Authorized |

Refresh

Controller time: 12/7/2007 13:30:47
Copyright 2000-2007 Fujitsu Siemens Computers

#### 6.2.4.3.5 Viewing each Port Access Control Statistics Page

**Selection Criteria**

**Port** - Selects the port to be displayed. When the selection is changed, a screen refresh will occur causing all fields to be updated for the newly selected port. All physical interfaces are valid.

**Non-Configurable Data**

**EAPOL Frames Received** - This displays the number of valid EAPOL frames of any type that have been received by this authenticator.

**EAPOL Frames Transmitted** - This displays the number of EAPOL frames of any type that have been transmitted by this authenticator.

**EAPOL Start Frames Received** - This displays the number of EAPOL start frames that have been received by this authenticator.

**EAPOL Logoff Frames Received** - This displays the number of EAPOL logoff frames that have been received by this authenticator.

**Last EAPOL Frame Version** - This displays the protocol version number carried in the most recently received EAPOL frame.

**Last EAPOL Frame Source** - This displays the source MAC address carried in the most recently received EAPOL frame.

**EAP Response/Id Frames Received** - This displays the number of EAP response/identity frames that have been received by this authenticator.

**EAP Response Frames Received** - This displays the number of valid EAP response frames (other than resp/id frames) that have been received by this authenticator.

**EAP Request/Id Frames Transmitted** - This displays the number of EAP request/identity frames that have been transmitted by this authenticator.

**EAP Request Frames Transmitted** - This displays the number of EAP request frames (other than request/identity frames) that have been transmitted by this authenticator.

**Invalid EAPOL Frames Transmitted** - This displays the number of EAPOL frames that have been received by this authenticator in which the frame type is not recognized.

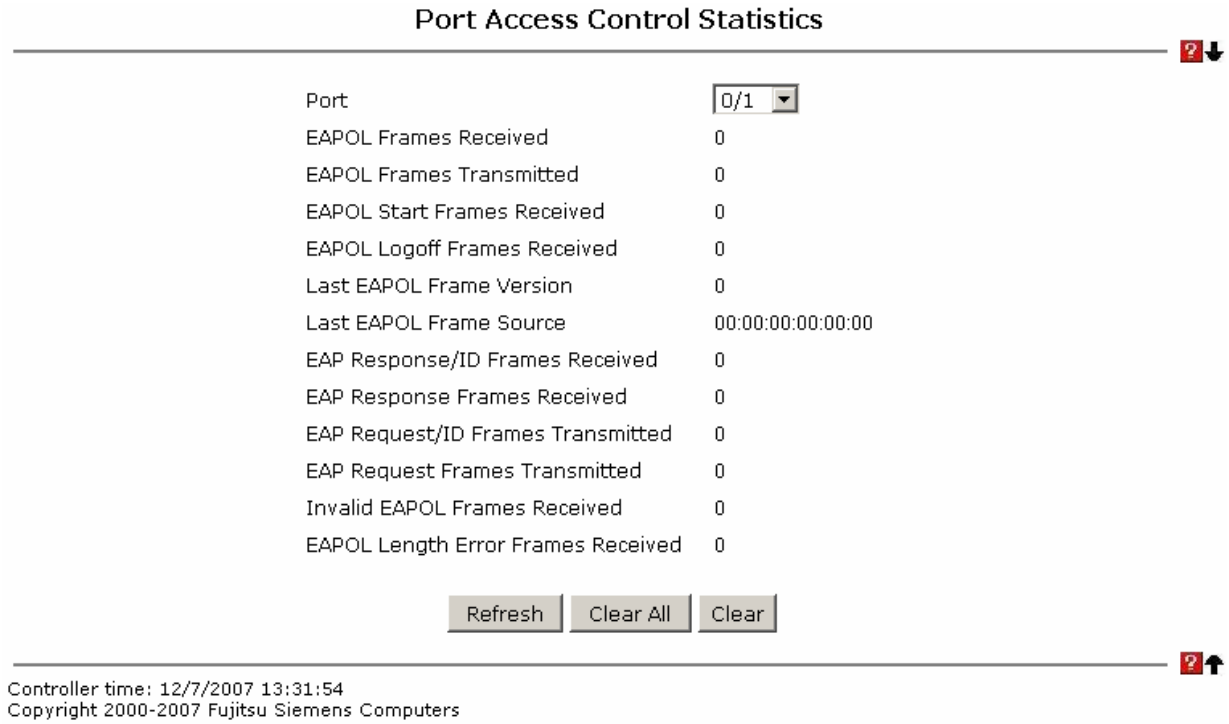
**EAP Length Error Frames Received** - This displays the number of EAPOL frames that have been received by this authenticator in which the frame type is not recognized.

**Command Buttons**

**Refresh** - Update the information on the page.

**Clear All** - This button resets all statistics for all ports to 0. There is no confirmation prompt. When this button is pressed, the stats are immediately cleared.

**Clear** - This button resets the statistics for the selected port. There is no confirmation prompt. When this button is pressed, the stats are immediately cleared.




### 6.2.4.3.6 Defining Access Control User Login Page

**Selection Criteria**

**Users** - Selects the user name that will use the selected login list for 802.1x port security.

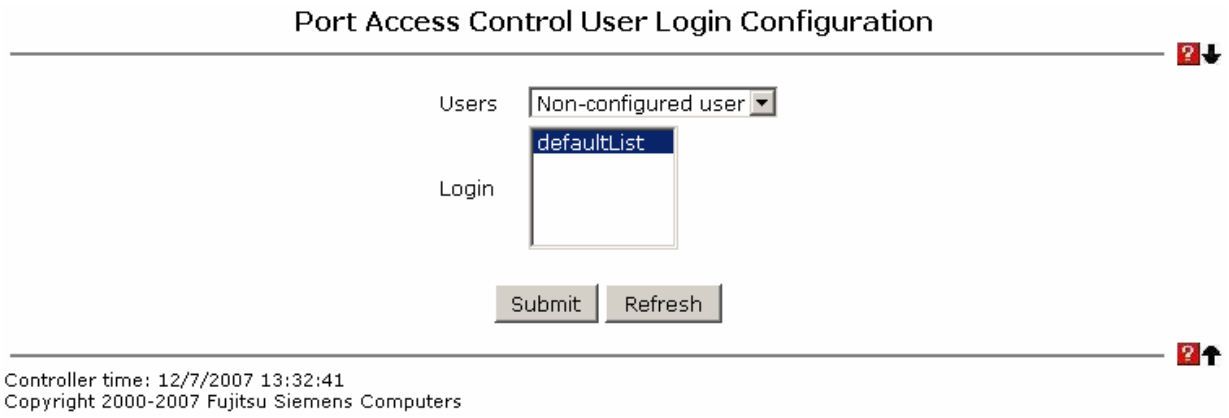
**Configurable Data**

**Login** - Selects the login to apply to the specified user. All configured logins are displayed.

**Command Buttons**

**Submit** - Sends the updated screen to the IBP and causes the changes to take effect on the IBP but these changes will not be retained across a power cycle unless a save is performed.

**Refresh** - Update the information on the page.



#### 6.2.4.3.7 Defining Each Port Access Privileges Page

**Selection Criteria**

**Port** - Selects the port to configure.

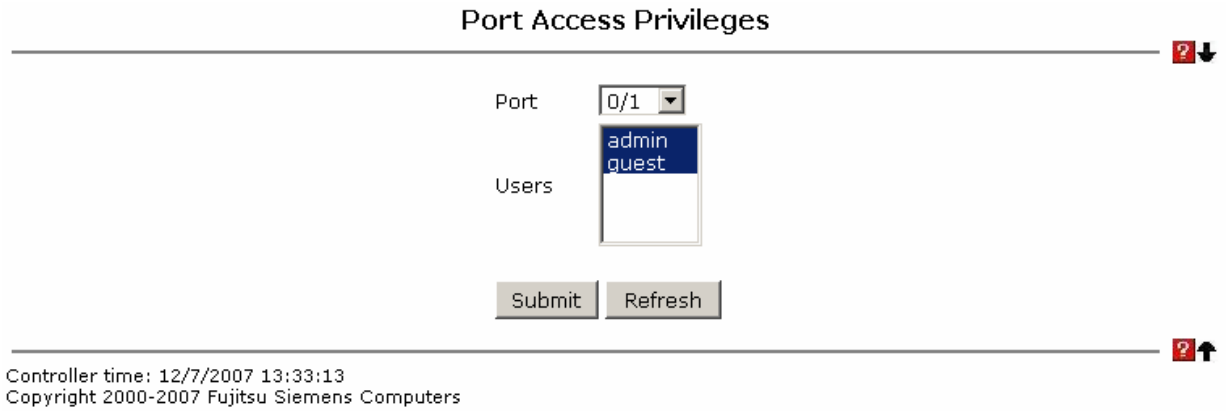
**Configurable Data**

**Users** - Selects the users that have access to the specified port or ports.

**Command Buttons**

**Submit** - Sends the updated screen to the IBP and causes the changes to take effect on the IBP but these changes will not be retained across a power cycle unless a save is performed.

**Refresh** - Update the information on the page.




#### 6.2.4.3.8 Viewing Each Port Access Privileges Summary Page

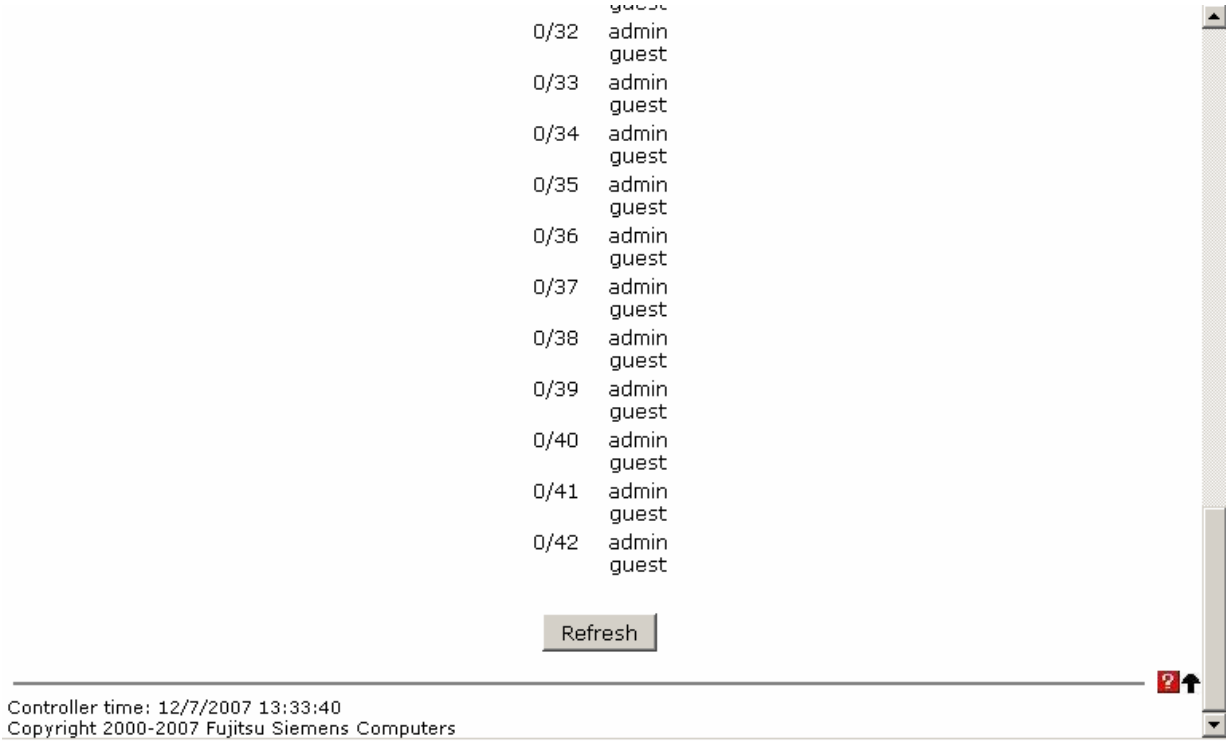
**Non-Configurable Data**

**Port** - Displays the port in Slot/Port format.

**Users** - Displays the users that have access to the port.

**Command Buttons**

**Refresh** - Update the information on the page.


0/32 admin guest
0/33 admin guest
0/34 admin guest
0/35 admin guest
0/36 admin guest
0/37 admin guest
0/38 admin guest
0/39 admin guest
0/40 admin guest
0/41 admin guest
0/42 admin guest
Refresh
Controller time: 12/7/2007 13:33:40
Copyright 2000-2007 Fujitsu Siemens Computers

### 6.2.4.4 Managing IP Filter

#### 6.2.4.4.1 IP Filter Configuration Page

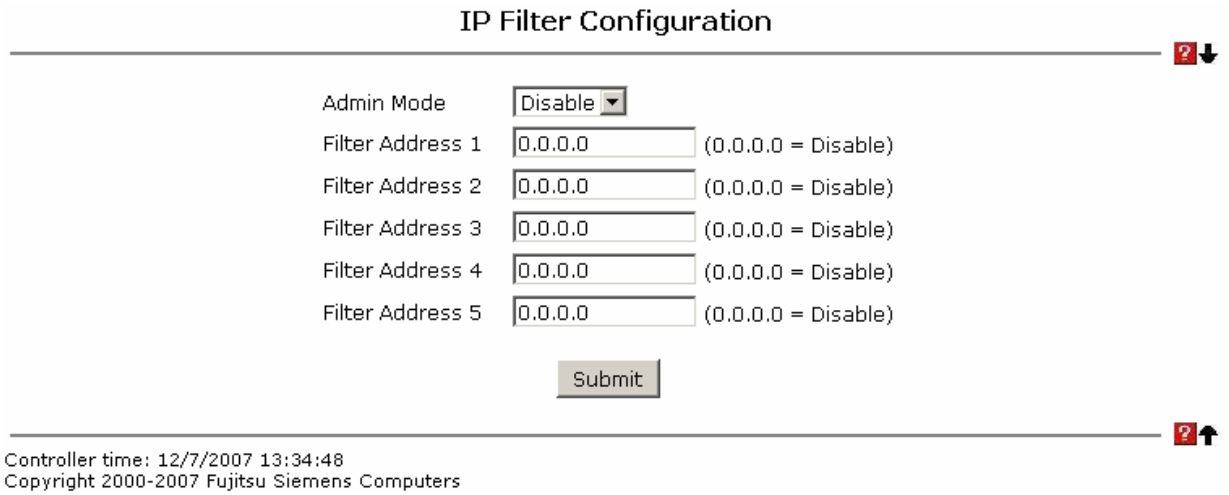
Management IP filter designates stations that are allowed to make configuration changes to the IBP. Select up to five management stations used to manage the IBP. If you choose to define one or more designated management stations, only the chosen stations, as defined by IP address, will be allowed management privilege through the web manager, Telnet session, Secure Shell (SSH) or Secure Socket Layer (SSL) for secure HTTP.

**Configurable Data**

**Filter Address 1~5** - Stations that are allowed to make configuration changes to the IBP.

**Command Buttons**

**Submit** - Send the updated screen to the IBP. Changes take effect on the IPB but these changes will not be retained across a power cycle unless a save is performed.



### 6.2.4.5 Managing Authentication Configuration

#### 6.2.4.5.1 Defining Authentication List Configuration Page

You use this screen to configure login lists. A login list specifies the authentication method(s) you want used to validate IBP or port access for the users associated with the list. The pre-configured users, admin and guest, are assigned to a pre-configured list named defaultList, which you may not delete. All newly created users are also assigned to the defaultList until you specifically assign them to a different list

**Selection Criteria**

**Authentication List** - Select the authentication login list you want to configure. Select 'create' to define a new login list. When you create a new login list, 'local' is set as the initial authentication method.

**Configurable Data**

**Authentication List Name** - If you are creating a new login list, enter the name you want to assign. It can be up to 15 alphanumeric characters and is not case sensitive.

**Method 1** - Use the dropdown menu to select the method that should appear first in the selected authentication login list. If you select a method that does not time out as the first method, such as 'local' no other method will be tried, even if you have specified more than one method. Note that this parameter will not appear when you first create a new login list. The options are:

**Local**- the user's locally stored ID and password will be used for authentication

**Radius**- the user's ID and password will be authenticated using the RADIUS server instead of locally

**Reject**- the user is never authenticated

**Tacacs**- the user's ID and password will be authenticated using the TACACS server instead of locally

**Undefined**- the authentication method is unspecified (this may not be assigned as the first method)

**Method 2** - Use the dropdown menu to select the method, if any, that should appear second in the selected authentication login list. This is the method that will be used if the first method times out. If you select a method that does not time out as the second method, the third method will not be tried. Note that this parameter will not appear when you first create a new login list.

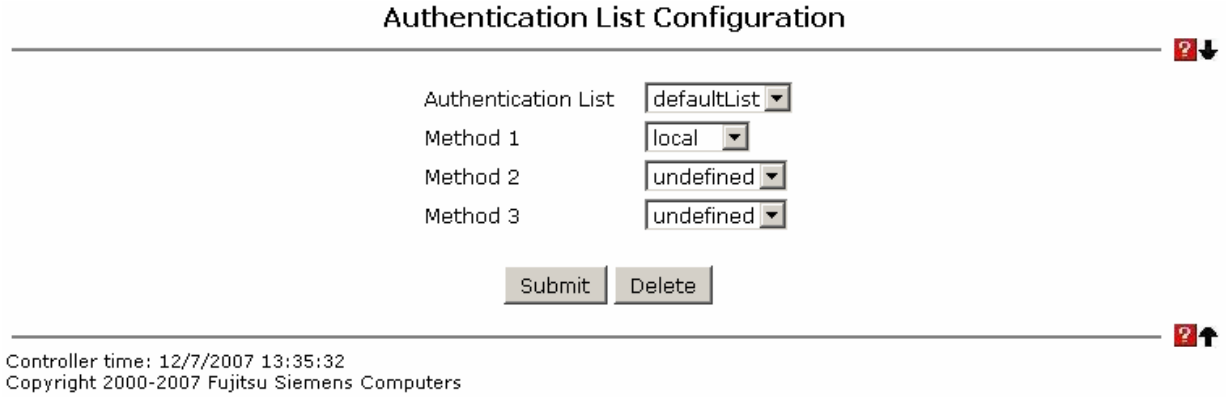
**Method 3** - Use the dropdown menu to select the method, if any, that should appear third in the selected authentication login list. Note that this parameter will not appear when you first create a new login list.

**Command Buttons**

**Submit** - Sends the updated screen to the IBP and causes the changes to take effect on the IBP. These changes will not be retained across a power cycle unless you perform a save.

**Delete** - Remove the selected authentication login list from the configuration. The delete will fail if the selected login list is assigned to any user (including the default user) for system login or IEEE 802.1x port access control. You can only use this button if you have Read/Write access. The change will not be retained across a power cycle unless you

perform a save.




#### 6.2.4.5.2 Viewing Authentication List Summary Page

**Non-Configurable Data**

**Authentication List** - Identifies the authentication login list summarized in this row.

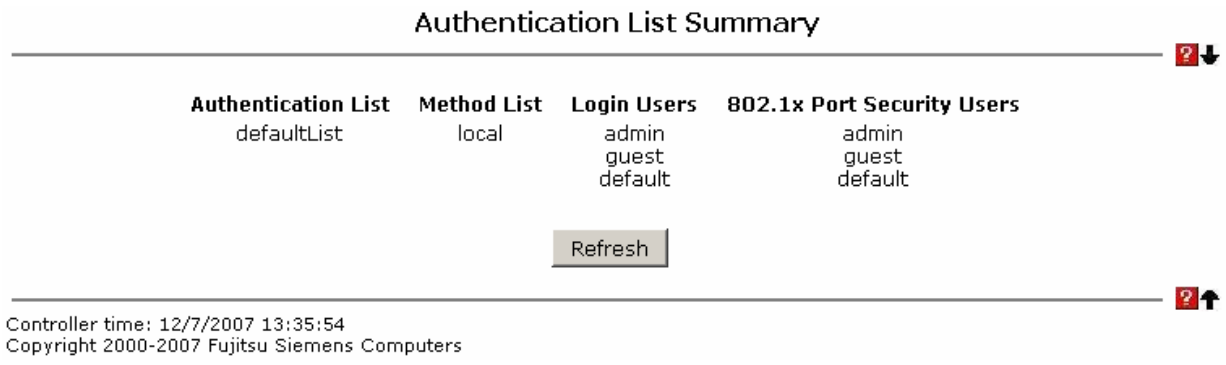
**Method List** - The ordered list of methods configured for this login list.

**Login Users** - The users you assigned to this login list on the User Login Configuration screen. This list is used to authenticate the users for system login access.

**802.1x Port Security Users** The users you assigned to this login list on the Port Access Control User Login Configuration screen - This list is used to authenticate the users for port access, using the IEEE 802.1x protocol.

**Command Buttons**

**Refresh** - Update the information on the page.




#### 6.2.4.5.3 Defining User Login Page

***Note: This page provides a user account (from those already created) to be added into the Authentication List.***

Each configured user is assigned to a login list that specifies how the user should be authenticated when attempting to access the IBP or a port on the IBP. After creating a new user account on the User Account screen, you should assign that user to a login list for the IBP using this screen and, if necessary, to a login list for the ports using the Port Access Control

User Login Configuration screen. If you need to create a new login list for the user, you would do so on the Login Configuration screen.

The pre-configured users, admin and guest, are assigned to a pre-configured list named defaultList, which you may not delete. All newly created users are also assigned to the defaultList until you specifically assign them to a different list.

A user that does not have an account configured on the IBP is termed the 'default' or 'non-configured' user. If you assign the 'non-configured user' to a login list that specifies authentication via the RADIUS server, you will not need to create an account for all users on each IBP. However, by default the 'non-configured user' is assigned to 'defaultList', which by default uses local authentication.

**Selection Criteria**

**User** - Select the user you want to assign to a login list. Note that you must always associate the admin user with the default list. This forces the admin user to always be authenticated locally to prevent full lockout from IBP's configuration. If you assign a user to a login list that requires remote authentication, the user's access to the IBP from all CLI, web, and telnet sessions will be blocked until the authentication is complete. Refer to the discussion of maximum delay in the RADIUS configuration help.

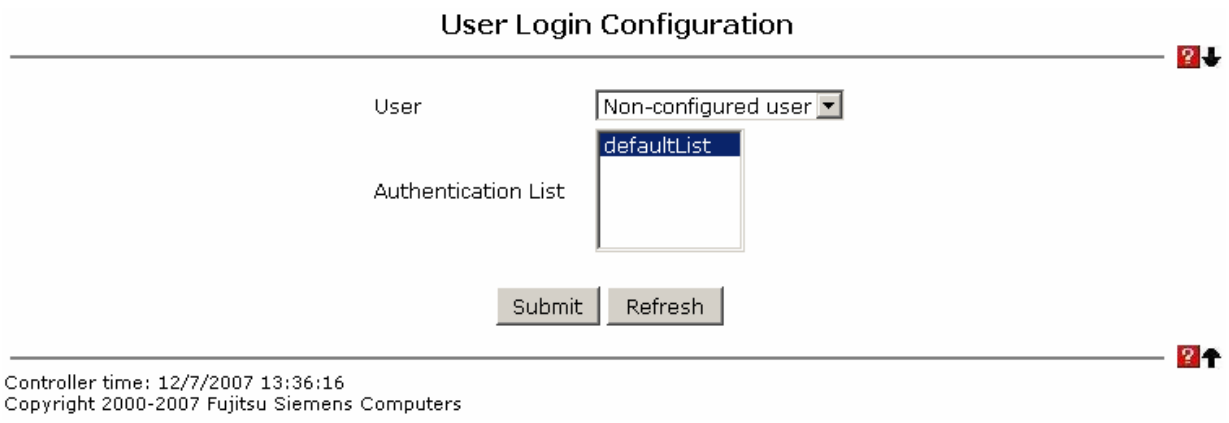
**Configurable Data**

**Authentication List** - Select the authentication login list you want to assign to the user for system login.

**Command Buttons**

**Submit** - Sends the updated screen to the IBP and causes the changes to take effect on the IBP. These changes will not be retained across a power cycle unless you perform a save.

**Refresh** - Updates the information on the page.



# 7 Command Reference

The Command Line Interface (CLI) syntax, conventions, and terminology are described in this section. Each CLI command is illustrated using the structure outlined below.

## 7.1 CLI Command Format

Commands are followed by values, parameters, or both.

**Example 1**
**ip address <ipaddr> <netmask> [<vlan-id>]**
• **Ip address** is the command name.
• **<ipaddr> <netmask>** are the required values for the command.
• **[<vlan-id>]** is the optional value for the command.

**Example 2**
**snmp-server host <loc>**
• **snmp-server location** is the command name.
• **<loc>** is the required parameter for the command.

**Example 3**

**clear port-group**
• **clear port-group** is the command name.

**Command**

The text in bold, non-italic font must be typed exactly as shown.

## 7.2 CLI Mode-based Topology

### Parameters

Parameters are order dependent.
The text in bold italics should be replaced with a name or number. To use spaces as part of a name parameter, enclose it in double quotes like this: "System Name with Spaces".

Parameters may be mandatory values, optional values, choices, or a combination.

– <parameter>. The <> angle brackets indicate that a mandatory parameter must be entered in place of the brackets and text inside them.

– [parameter]. The [] square brackets indicate that an optional parameter may be entered in place of the brackets and text inside them.

– choice1 | choice2. The | indicates that only one of the parameters should be entered. The {} curly braces indicate that a parameter must be chosen from the list of choices.

### Values

**ipaddr** This parameter is a valid IP address, made up of four decimal bytes ranging from 0 to 255. The default for all IP parameters consists of zeros (that is, 0.0.0.0). The interface IP address of 0.0.0.0 is invalid.

**macaddr** The MAC address format is six hexadecimal numbers separated by colons, for example 00:06:29:32:81:40.

**slot/port** This parameter denotes a valid slot number, and a valid port number. For example, 0/1 represents slot number 0 and port number 1. The <slot/port> field is composed of a valid slot number and a valid port number separated by a forward slash (/).

**logical slot/port** This parameter denotes logical slot number, and logical port number assigned. This is applicable in the case of a port-channel (LAG). The operator can use the logical logical slot number, and the logical port number to configure the port-channel.

### Conventions

Network addresses are used to define a link to a remote host, workstation, or network. Network addresses are shown using the following syntax:

**Table 5-1. Network Address Syntax**

| Address Type | Format | Range |
|---|---|---|
| IPAddr | A.B.C.D | 0.0.0.0 to 255.255.255.255 |
| MacAddr | YY:YY:YY:YY:YY:YY | hexidecimal digit pairs |

Double quotation marks such as "System Name with Spaces" set off user defined strings. If the operator wishes to use spaces as part of a name parameter then it must be enclosed in double quotation marks.

Empty strings (““) are not valid user defined strings. Command completion finishes spelling the command when enough letters of a command are typed to uniquely identify the command word. The command may be executed by typing <enter> (command abbreviation) or the command word may be completed by typing the <tab> or <space bar> (command completion).

The value 'Err' designates that the requested value was not internally accessible. This should never happen and indicates that there is a case in the software that is not handled correctly.

The value of '-----' designates that the value is unknown.

### Annotations

The CLI allows the user to type single-line annotations at the command prompt for use when writing test or configuration scripts and for better readability. The exclamation point (‘!’) character flags the beginning of a comment. The comment flag character can begin a word anywhere on the command line and all input following this character is ignored. Any command line that begins with the character ‘!’ is recognized as a comment line and ignored by the parser.

Some examples are provided below:

**! Script file for displaying the ip interface**
**! Display information about interfaces**
**show ip interface 0/1 !Displays the information about the first interface**
**! Display information about the next interface**
**show ip interface 0/2**
**! End of the script file**

## 7.3 System Information and Statistics commands

### 7.3.1 show arp

This command displays connectivity between the IBP and other devices. The Address Resolution Protocol (ARP) cache identifies the MAC addresses of the IP stations communicating with the IBP.

**Syntax**

**show arp**

**Default Setting**

None

**Command Mode**

Privileged Exec

**Display Message**

**MAC Address:** A unicast MAC address for which the IBP has forwarding and/or filtering information. The format is 6 two-digit hexadecimal numbers that are separated by colons. For example: 00:23:45:67:89:AB
**IP Address:** The IP address assigned to each interface.
**Interface:** Valid slot number and a valid port number.

### 7.3.2 show calendar

This command displays the system clock.

**Syntax**

**show calendar**

**Default Setting**

None

**Command Mode**

Privileged Exec

**Display Message**

**Current Time** displays system time

### 7.3.3 show eventlog

This command displays the event log, which contains error messages from the system, in the Primary Management System . The event log is not cleared on a system reset.

| **Syntax** |
| --- |
| **show eventlog** |

**Default Setting**

None

**Command Mode**

Privileged Exec

**Display Message**

**File:** The file in which the event originated.
**Line:** The line number of the event.
**Task Id:** The task ID of the event.
**Code:** The event code.
**Time:** The time this event occurred.

**Note:** Event log information is retained across a system reset.

### 7.3.4 show running-config

This command is used to display/capture the current setting of different protocol packages supported on IBP. This command displays/captures only commands with settings/configurations with values that differ from the default value. The output is displayed in script format, which can be used to configure another IBP with the same configuration. When a script name is provided, the output is redirected to a configuration script. The option [all] will also enable the display/capture of all commands with settings/configurations that include values that are same as the default values. If the optional <scriptname> is provided with a file

name extension of ".scr", the output will be redirected to a script file.

**Syntax**

**show running-config [all] [<scriptname>]**

**[all] -** enable the display/capture of all commands with settings/configurations that include values that are same as the default values.

**<scriptname> -** redirect the output to the file <scriptname>.

**Default Setting**

None

**Command Mode**

Privileged Exec

### 7.3.5 show sysinfo

This command displays IBP brief information and MIBs supported.

**Syntax**

**show sysinfo**

**Default Setting**

None

**Command Mode**

Privileged Exec

**Display Message**

**System Description:** The text used to identify this IBP.
**System Name:** The name used to identify the IBP.
**System Location:** The text used to identify the location of the IBP. May be up to 31 alpha-numeric characters. The factory default is blank.
**System Contact:** The text used to identify a contact person for this IBP. May be up to 31 alphanumeric characters. The factory default is blank.
**System Object ID:** The manufacturing ID.
**System Up Time:** The time in days, hours and minutes since the last IBP reboot.
**MIBs Supported:** A list of MIBs supported by this agent.

### 7.3.6 show system

This command displays IBP system information.

**Syntax**

**show system**

**Default Setting**

None

**Command Mode**

Privileged Exec

**Display Message**

**System Description:** Text used to identify this IBP.
**System Object ID:** The manufacturing ID
**System Information**
**System Up Time:** The time in days, hours and minutes since the last IBP reboot.
**System Name:** Name used to identify the IBP.
**System Location:** Text used to identify the location of the IBP. May be up to 31 alpha-numeric characters. The factory default is blank.
**System Contact:** Text used to identify a contact person for this IBP. May be up to 31 alphanumeric characters. The factory default is blank.
**MAC Address:** The burned in MAC address used for in-band connectivity.
**Web Server:** Displays to enable/disable web server function
**Web Server Port:** Displays the web server http port. The factory default is 80.
**Web Server Java Mode:** Specifies if the IBP should allow access to the Java applet in the header frame. Enabled means the applet can be viewed. The factory default is enabled.
**Protocol Current:** Indicates which network protocol is being used. The options are bootp | dhcp | none.
**DHCP Client Identifier TEXT:** DCHP client identifier for this IBP.

### 7.3.7 show hardware

This command displays inventory information for the IBP.

**Syntax**

**show hardware**

**Default Setting**

None

**Command Mode**

Privileged Exec

**Display Message**

**System Description:** Text used to identify the product name of this IBP.
**Machine Type:** Specifies the machine model as defined by the Vital Product Data.
**Machine Model:** Specifies the machine model as defined by the Vital Product Data.
**Serial Number:** The unique box serial number for this IBP.
**Label Revision Number:** The label revision serial number of this IBP is used for manufacturing purposes.
**Part Number:** Manufacturing part number.
**Hardware Version:** The hardware version of this IBP. It is divided into four parts. The first byte is the major version and the second byte represents the minor version.
**Loader Version:** The release version maintenance number of the loader code currently running on the IBP. For example, if the major version was 2, and the minor version was 4, the format would be '2.4'.
**Boot Rom Version:** The release version maintenance number of the boot ROM code currently running on the IBP. For example, if the major version was 2, and the minor version was 4, the format would be '2.4'.
**Operating Code Version:** The release version maintenance number of the code currently running on the IBP. For example, if the major version was 2, and the minor version was 4, the format would be '2.4'.
**Additional Packages:** This displays the additional packages that are incorporated into this system.

### 7.3.8 show version

This command displays version information for the IBP.

**Syntax**

**show version**

**Default Setting**

None

**Command Mode**

Privileged Exec

**Display Message**

**Serial Number:** The unique box serial number for this IBP.
**Hardware Version:** The hardware version of this IBP. It is divided into two parts. The first byte is the major version and the second byte represents the minor version.
**Software Version:** The release version number of the code currently running on the IBP.
**Label Revision Number:** The label revision serial number of this IBP is used for manufacturing purpose.
**Part Number:** Manufacturing part number.
**Machine Model:** The model within the machine type.
**Loader Version:** The release version maintenance number of the loader code currently

running on the IBP. For example, if the major version was 2 and the minor version was 4, the format would be '2.4'.
**Operating Code Version:** The release version maintenance number of the code currently running on the IBP. For example, if the major version was 2 and the minor version was 4, the format would be '2.4'.
**Boot Rom Version:** The release version maintenance number of the boot rom code currently running on the IBP. For example, if the major version was 2 and the minor version was 4, the format would be '2.4'.

### 7.3.9 show loginsession

This command displays current telnet and serial port connections to the IBP.

| Syntax |
| --- |
| **show loginsession** |

**Default Setting**

None

**Command Mode**

Privileged Exec

**Display Message**

**ID:** Login Session ID
**User Name:** The name the user will use to login using the serial port or Telnet. A new user may be added to the IBP by entering a name in a blank entry. The user name may be up to 8 characters, and is not case sensitive. Two users are included as the factory default, admin, and guest.
**Connection From:** IP address of the telnet client machine or EIA-232 for the serial port connection.
**Idle Time:** Time this session has been idle.
**Session Time:** Total time this session has been connected.
**Session Type:** Shows the type of session: telnet, serial or SSH.

## 7.4 Device Configuration Commands

### 7.4.1 Interface

#### 7.4.1.1 show interface status

This command displays the Port monitoring information for the system.

**Syntax**

**show interface status {<slot/port> | all}**

**<slot/port> -** is the desired interface number.

**all -** This parameter displays information for all interfaces.

**Default Setting**

None

**Command Mode**

Privileged Exec

**Display Message**

**Intf:** The physical slot and physical port.
**Type:** If not blank, this field indicates that this port is a special type of port. The possible values are:
**PC Mbr** - This port is a member of a port-channel (LAG).

**Admin Mode:** Selects the Port control administration state. The port must be enabled in order for it to be allowed into the network. – It may be enabled or disabled. The factory default is enabled.
**Physical Mode:** Selects the desired port speed and duplex mode. If auto-negotiation support is selected, then the duplex mode and speed will be set from the auto-negotiation process. Note that the port's maximum capability (full duplex -100M) will be advertised. Otherwise, this object will determine the port's duplex mode and transmission rate. The factory default is Auto.
**Physical Status:** Indicates the port speed and duplex mode.
**Link Status:** Indicates whether the Link is up or down.
**Link Trap:** This object determines whether to send a trap when link status changes. The factory default is enabled.
**Flow Mode:** Displays flow control mode.
**Capabilities Status:** Displays interface capabilities.

#### 7.4.1.2 show interface

This command displays the Port monitoring information for the system.

**Syntax**

**show interface <slot/port>**

**<slot/port> -** is the desired interface number.

**Default Setting**

None

**Command Mode**

Privileged Exec

**Display Message**

**Intf:** The physical slot and physical port.
**Type:** If not blank, this field indicates that this port is a special type of port. The possible values are:
**PC Mbr** - This port is a member of a port-channel (LAG).
**Description:** This description of a port.
**Admin Mode:** Selects the Port control administration state. The port must be enabled in order for it to be allowed into the network. – It may be enabled or disabled. The factory default is enabled.
**Physical Mode:** Selects the desired port speed and duplex mode. If auto-negotiation support is selected, then the duplex mode and speed will be set from the auto-negotiation process. Note that the port's maximum capability (full duplex -100M) will be advertised. Otherwise, this object will determine the port's duplex mode and transmission rate. The factory default is Auto.
**Physical Status:** Indicates the port speed and duplex mode.
**Link Status:** Indicates whether the Link is up or down.
**Link Trap:** This object determines whether to send a trap when link status changes. The factory default is enabled.
**Flow Mode:** Displays flow control mode.
**Capabilities Status:** Displays interface capabilities.

#### 7.4.1.3 show interface counters

This command displays a summary of statistics for a specific interface or all interfaces.

**Syntax**

**show interface counters {<slot/port> | all}**

**<slot/port> -** is the desired interface number.

**all -** This command displays statistics information for all interfaces.

**Default Setting**

None

**Command Mode**

Privileged Exec

**Display Message**

The display parameters when the argument is '<slot/port>' are as follows:

**Packets Received Without Error:** The total number of packets (including broadcast packets and multicast packets) received by the processor.
**Packets Received With Error:** The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
**Broadcast Packets Received:** The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.
**Packets Transmitted Without Error:** The total number of packets transmitted out of the interface.
**Transmit Packets Errors:** The number of outbound packets that could not be transmitted because of errors.
**Collisions Frames:** The best estimate of the total number of collisions on this Ethernet segment.
**Time Since Counters Last Cleared:** The elapsed time, in days, hours, minutes, and seconds since the statistics for this port were last cleared.

The display parameters when the argument is 'all' are as follows:

**Interface:** The physical slot and physical port or the logical slot and logical port.
**Summary:** The summation of the statistics of all ports.
**Packets Received Without Error:** The total number of packets (including broadcast packets and multicast packets) received.
**Packets Received With Error:** The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
**Broadcast Packets Received:** The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.
**Packets Transmitted Without Error:** The total number of packets transmitted.
**Transmit Packets Errors:** The number of outbound packets that could not be transmitted because of errors.
**Collisions Frames:** The best estimate of the total number of collisions on this Ethernet segment.

This command displays detailed statistics for a specific port or for all CPU traffic based upon the argument.

**Syntax**

**show interface counters detailed {<slot/port> | switchport}**

**<slot/port> -** is the desired interface number.

**switchport -** This parameter specifies whole IBP or all interfaces.

**Default Setting**

None

**Command Mode**

Privileged Exec

**Display Message**

The display parameters when the argument is ' <slot/port>' are as follows:

**Total Packets Received (Octets):** The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets). This object can be used as a reasonable estimate of Ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval. The result of this equation is the value Utilization which is the percent utilization of the Ethernet segment on a scale of 0 to 100 percent.
**Packets Received 64 Octets:** The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).
**Packets Received 65-127 Octets:** The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
**Packets Received 128-255 Octets:** The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
**Packets Received 256-511 Octets:** The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
**Packets Received 512-1023 Octets:** The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
**Packets Received 1024-1518 Octets:** The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).
**Packets Received > 1522 Octets:** The total number of packets received that were longer than 1522 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
**Packets RX and TX 64 Octets:** The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).
**Packets RX and TX 65-127 Octets:** The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
**Packets RX and TX 128-255 Octets:** The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
**Packets RX and TX 256-511 Octets:** The total number of packets (including bad packets)

received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).

**Packets RX and TX 512-1023 Octets:** The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).

**Packets RX and TX 1024-1518 Octets:** The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).

**Packets RX and TX 1519-1522 Octets:** The total number of packets (including bad packets) received that were between 1519 and 1522 octets in length inclusive (excluding framing bits but including FCS octets).

**Packets RX and TX 1523-2047 Octets:** The total number of packets (including bad packets) received that were between 1523 and 2047 octets in length inclusive (excluding framing bits but including FCS octets).

**Packets RX and TX 2048-4095 Octets:** The total number of packets (including bad packets) received that were between 2048 and 4095 octets in length inclusive (excluding framing bits but including FCS octets).

**Packets RX and TX 4096-9216 Octets:** The total number of packets (including bad packets) received that were between 4096 and 9216 octets in length inclusive (excluding framing bits but including FCS octets).

**Total Packets Received Without Errors**

**Unicast Packets Received:** The number of subnetwork-unicast packets delivered to a higher-layer protocol.

**Multicast Packets Received:** The total number of good packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.

**Broadcast Packets Received:** The total number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets.

**Total Packets Received with MAC Errors**

**Jabbers Received:** The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). Note that this definition of jabber is different than the definition in IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). These documents define jabber as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms.

**Undersize Received:** The total number of packets received that were less than 64 octets in length with GOOD CRC(excluding framing bits but including FCS octets).

**Fragments Received:** The total number of packets received that were less than 64 octets in length with ERROR CRC(excluding framing bits but including FCS octets).

**Alignment Errors:** The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad FCS with a non-integral number of octets.

**FCS Errors:** The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad FCS with an integral number of octets

**Overruns:** The total number of frames discarded as this port was overloaded with incoming packets, and could not keep up with the inflow.

**Total Packets Transmitted (Octets)**

**Packets Transmitted 64 Octets:** The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).

**Packets Transmitted 65-127 Octets:** The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
**Packets Transmitted 128-255 Octets:** The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
**Packets Transmitted 256-511 Octets:** The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
**Packets Transmitted 512-1023 Octets:** The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
**Packets Transmitted 1024-1518 Octets:** The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).
**Packets Transmitted 1519-1522 Octets:** The total number of packets (including bad packets) received that were between 1519 and 1522 octets in length inclusive (excluding framing bits but including FCS octets).
**Max Info:** The maximum size of the Info (non-MAC) field that this port will receive or transmit.

**Total Packets Transmitted Successfully**
**Unicast Packets Transmitted:** The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
**Multicast Packets Transmitted:** The total number of packets that higher-level protocols requested be transmitted to a Multicast address, including those that were discarded or not sent.
**Broadcast Packets Transmitted:** The total number of packets that higher-level protocols requested be transmitted to the Broadcast address, including those that were discarded or not sent.

**Total Transmit Errors**
**FCS Errors:** The total number of packets transmitted that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad FCS with an integral number of octets
**Tx Oversized:** The total number of frames that exceeded the max permitted frame size. This counter has a max increment rate of 815 counts per sec. at 10 Mb/s.
**Underrun Errors:** The total number of frames discarded because the transmit FIFO buffer became empty during frame transmission.

**Total Transmited Packets Discards**
**Single Collision Frames:** A count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision.
**Multiple Collision Frames:** A count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision.
**Excessive Collisions:** A count of frames for which transmission on a particular interface fails due to excessive collisions.

**EAPOL Frames Received:** The number of valid EAPOL frames of any type that have been received by this authenticator.
**EAPOL Frames Transmitted:** The number of EAPOL frames of any type that have been transmitted by this authenticator.
**Time Since Counters Last Cleared:** The elapsed time, in days, hours, minutes, and

seconds since the statistics for this port were last cleared.

The display parameters when the argument is ‘switchport’ are as follows:

**Total Packets Received (Octets):** The total number of octets of data received by the processor (excluding framing bits but including FCS octets).
**Packets Received Without Error:** The total number of packets (including broadcast packets and multicast packets) received by the processor.
**Unicast Packets Received:** The number of subnetwork-unicast packets delivered to a higher-layer protocol.
**Multicast Packets Received:** The total number of packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.
**Broadcast Packets Received:** The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.
**Receive Packets Discarded:** The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.

**Octets Transmitted:** The total number of octets transmitted out of the interface, including framing characters.
**Packets Transmitted without Errors:** The total number of packets transmitted out of the interface.
**Unicast Packets Transmitted:** The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
**Multicast Packets Transmitted:** The total number of packets that higher-level protocols requested be transmitted to a Multicast address, including those that were discarded or not sent.
**Broadcast Packets Transmitted:** The total number of packets that higher-level protocols requested be transmitted to the Broadcast address, including those that were discarded or not sent.
**Transmit Packets Discarded:** The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.

**Most Address Entries Ever Used:** The highest number of Forwarding Database Address Table entries that have been learned by this IBP since the most recent reboot.
**Address Entries Currently in Use:** The number of Learned and static entries in the Forwarding Database Address Table for this IBP.

**Time Since Counters Last Cleared:** The elapsed time, in days, hours, minutes, and seconds, since the statistics for this IBP were last cleared.

#### 7.4.1.4 show interface IBP

This command displays a summary of statistics for all CPU traffic.

**Syntax**

**show interface switch**

**Default Setting**

None

**Command Mode**

Privileged Exec

**Display Message**

**Packets Received Without Error:** The total number of packets (including broadcast packets and multicast packets) received by the processor.
**Broadcast Packets Received:** The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.
**Packets Received With Error:** The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
**Packets Transmitted Without Error:** The total number of packets transmitted out of the interface.
**Broadcast Packets Transmitted:** The total number of packets that higher-level protocols requested to be transmitted to the Broadcast address, including those that were discarded or not sent.
**Transmit Packet Errors:** The number of outbound packets that could not be transmitted because of errors.
**Address Entries Currently In Use:** The total number of Forwarding Database Address Table entries now active on the IBP, including learned and static entries.
**Time Since Counters Last Cleared:** The elapsed time, in days, hours, minutes, and seconds since the statistics for this IBP were last cleared.

#### 7.4.1.5 interface

This command is used to enter Interface configuration mode.

**Syntax**

**interface <slot/port>**

**<slot/port> -** is the desired interface number.

**Default Setting**

None

**Command Mode**

Global Config

#### 7.4.1.6 interface range

This command is used to enter Interface range configuration mode.

**Syntax**

. **interface range {<slot/port> [ - <slot/port>]} [, {<slot/port> [ - <slot/port>]} [, {<slot/port> [ - <slot/port>]} [, {<slot/port> [ - <slot/port>]} [, {<slot/port> [ - <slot/port>]}]]]]**

**<slot/port> -** is the desired interface number.

**Default Setting**

None

**Command Mode**

Global Config

#### 7.4.1.7 speed-duplex

This command is used to set the speed and duplex mode for the interface.

**Syntax**

**speed-duplex {10 | 100} {full-duplex | half-duplex}**

**100 -** 100BASE-T
**10 -** 10BASE-T
**full-duplex -** Full duplex
**half-duplex -** Half duplex

**Default Setting**

None

**Command Mode**

Interface Config

This command is used to set the speed and duplex mode for all interfaces.

**Syntax**

**Speed-duplex all {10 | 100} {full-duplex | half-duplex}**

**100 -** 100BASE-T
**10 -** 10BASE-T
**full - duplex -** Full duplex
**half - duplex -** Half duplex
**all -** This command represents all interfaces.

**Default Setting**

None

**Command Mode**

Global Config

#### 7.4.1.8 negotiate

This command enables automatic negotiation on a port. The default value is enabled.

**Syntax**

**negotiate**

**no negotiate**

**no -** This command disables automatic negotiation on a port.

**Default Setting**

Enable

**Command Mode**

Interface Config

This command enables automatic negotiation on all interfaces. The default value is enabled.

**Syntax**

**negotiate all**

**no negotiate all**

**all -** This command represents all interfaces.
**no -** This command disables automatic negotiation on all interfaces.

**Default Setting**

Enable

**Command Mode**

Global Config

### 7.4.1.9 capabilities

This command is used to set the capabilities on specific interface.

**Syntax**

**capabilities {{10 | 100 } {full-duplex | half-duplex}} | {1000 full-duplex }**

**no capabilities {{10 | 100 } {full-duplex | half-duplex}} | {1000 full-duplex }**

**10 -** 10BASE-T
**100 -** 100BASE-T
**1000 -** 1000BASE-T
**full-duplex -** Full duplex
**half-duplex -** Half duplex
**no -** This command removes the advertised capability with using parameter.

**Default Setting**

10 half-duplex, 10 full-duplex, 100 half-duplex, 100 full-duplex, and 1000 full-duplex

**Command Mode**

Interface Config

This command is used to set the capabilities on all interfaces.

**Syntax**

**capabilities all {{10 | 100} {full-duplex | half-duplex}} | {1000 full-duplex }**

**no capabilities all {{10 | 100} {full-duplex | half-duplex}} | {1000 full-duplex }**

**10 -** 10BASE-T
**100 -** 100BASE-T
**1000 -** 1000BASE-T
**full-duplex -** Full duplex
**half-duplex -** Half duplex
**all -** This command represents all interfaces.
**no -** This command removes the advertised capability with using parameter

**Default Setting**

10 half-duplex, 10 full-duplex, 100 half-duplex, 100 full-duplex, and 1000 full-duplex

**Command Mode**

Global Config

### 7.4.1.10 description

This command is used to add a description for the interface.

**Syntax**

**description <string>**

**<dtring> -** Up to 64 characters describing this interface.

**Default Setting**

None

**Command Mode**

Interface Config

### 7.4.1.11 storm-control flowcontrol

This command enables 802.3x flow control for all interfaces on the IBP.

**Note:** This command only applies to full-duplex mode ports.

**Syntax**

**storm-control flowcontrol**
**no storm-control flowcontrol**

**no -** This command disables 802.3x flow control for all interfaces on the IBP.

**Default Setting**

Disabled

**Command Mode**

Global Config

This command enables 802.3x flow control for the specific interface.

**Note:** This command only applies to full-duplex mode ports.

**Syntax**

**storm-control flowcontrol**

**no storm-control flowcontrol**

**no -** This command disables 802.3x flow control for the specific interface.

**Default Setting**

Disabled

**Command Mode**

Interface Config

### 7.4.2 L2 MAC Address and Multicast Forwarding Database Tables

#### 7.4.2.1 show mac-addr-table

This command displays the forwarding database entries. If the command is entered with no parameter, the entire table is displayed. This is the same as entering the optional **all** parameter. Alternatively, the administrator can enter a MAC Address to display the table entry for the requested MAC address and all entries following the requested MAC address.

**Syntax**

**show mac-addr-table [{<macaddr> |all}]**

**<macaddr> -** enter a MAC Address to display the table entry for the requested MAC address.

**all –** this command displays the entire table.

**Default Setting**

None

**Command Mode**

Privileged Exec

**Display Message**

**Mac Address:** A unicast MAC address for which the IBP has forwarding and/or filtering

information. The format is 6 or 8 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB. In an IVL system the MAC address will be displayed as 8 bytes. In an SVL system, the MAC address will be displayed as 6 bytes. **Note: This software version only supports IVL systems.**
**Interface:** The port on which this L2 MAC address was learned.
**if Index:** This object indicates the if Index of the interface table entry associated with this port.
**Status:** The status of this entry.
The meanings of the values are:
**Static:** The value of the corresponding instance was added by the system or a user when a static MAC filter was defined. It cannot be relearned.
**Learned:** The value of the corresponding instance was learned by observing the source MAC addresses of incoming traffic, and is currently in use.
**Management:** The value of the corresponding instance (system MAC address) is also the value of an existing instance of dot1dStaticAddress. It is identified with interface 3/1.
**Self:** The value of the corresponding instance is the address of one of the IBP's physical interfaces (the system's own MAC address).
**Other:** The value of the corresponding instance does not fall into one of the other categories.

#### 7.4.2.2 show mac-address-table igmpsnooping

This command displays the IGMP Snooping entries in the Multicast Forwarding Database (MFDB) table.

**Syntax**

**show mac-address-table igmpsnooping**

**Default Setting**

None

**Command Mode**

Privileged Exec

**Display Message**

**Mac Address:** A unicast MAC address for which the IBP has forwarding and/or filtering information. The format is 6 or 8 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB. In an IVL system the MAC address will be displayed as 8 bytes. In an SVL system, the MAC address will be displayed as 6 bytes. **Note: This software version only supports IVL systems.**
**Type:** This displays the type of the entry. Static entries are those that are configured by the end user. Dynamic entries are added to the table as a result of a learning process or protocol.
**Description:** The text description of this multicast table entry.
**Interfaces:** The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

### 7.4.2.3 show mac-address-table multicast

This command displays the MFDB information. If the command is entered with no parameter, the entire table is displayed. This is the same as entering the *all* parameter. The user can display the table entry for one MAC Address by specifying the MAC address as an optional parameter.

**Syntax**

**show mac-address-table multicast {<macaddr> <vlanid> | all }**

**<macaddr> -** enter a MAC Address to display the table entry for the requested MAC address

**<vlanid> -** VLAN ID (Range: 1 – 4094)

**all –** This command displays the entire table.

**Default Setting**

None

**Command Mode**

Privileged Exec

**Display Message**

**Mac Address:** A unicast MAC address for which the IBP has forwarding and/or filtering information. The format is 6 or 8 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB. In an IVL system the MAC address will be displayed as 8 bytes. In an SVL system, the MAC address will be displayed as 6 bytes. **Note: This software version only supports IVL systems.**
**Type:** This displays the type of the entry. Static entries are those that are configured by the end user. Dynamic entries are added to the table as a result of a learning process or protocol.
**Source:** The component that is responsible for this entry in the Multicast Forwarding Database. Possible values are IGMP Snooping, and Static Filtering.
**Description:** The text description of this multicast table entry.
**Interfaces:** The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).
**Forwarding Interfaces:** The resultant forwarding list is derived from combining all the component's forwarding interfaces and removing the interfaces that are listed as the static filtering interfaces.

#### 7.4.2.4 show mac-address-table stats

This command displays the MFDB statistics.

**Syntax**

**show mac-address-table stats**

**Default Setting**

None

**Command Mode**

Privileged Exec

**Display Message**

**Max MFDB Table Entries:** This displays the total number of entries that can possibly be in the MFDB.
**Most MFDB Entries Since Last Reset:** This displays the largest number of entries that have been present in the Multicast Forwarding Database table. This value is also known as the MFDB high-water mark.
**Current Entries:** This displays the current number of entries in the Multicast Forwarding Database table.

#### 7.4.2.5 show mac-address-table agetime

This command displays the forwarding database address aging timeout.

**Syntax**

**show mac-address-table agetime**

**Default Setting**

None

**Command Mode**

Privileged Exec

**Display Message**

**Address Aging Timout:** This displays the total number of seconds for Forwarding Database table.

#### 7.4.2.6 mac-address-table aging-time

This command configures the forwarding database address aging timeout in seconds.

**Syntax**

**mac-address-table aging-time <10-1000000>**

**no mac-address-table aging-time <10-1000000>**

**<10-1000000> -** aging-time (Range: 10-1000000) in seconds
**no -** This command sets the forwarding database address aging timeout to 300 seconds.

**Default Setting**

300

**Command Mode**

Global Config

### 7.4.3 IGMP Snooping

#### 7.4.3.1 Show Commands

##### 7.4.3.1.1 show igmp snooping

This command displays IGMP Snooping information.

**Syntax**

**show igmpsnooping [<uplinkSetName>]**

**Default Setting**

None

**Command Mode**

Privileged Exec

**Display Message**

**Uplink Set Name:** This indicates the name of uplink set
**IGMP Snooping:** This displays the IGMP snooping is enabled or disabled.

#### 7.4.3.2 Configuration Commands

##### 7.4.3.2.1 igmpsnooping

This command enables IGMP Snooping on a Uplink Set. The default value is enabled.

**Syntax**

**igmpsnooping <uplinkSetName>**

**no igmpsnooping <uplinkSetName>**

**<uplinkSetName> -** The name of a uplink set which the IGMP snooping to be enabled or disabled.
**no -** This command disables IGMP Snooping on the specific uplink set.

**Default Setting**

Disabled

**Command Mode**

Global Config

### 7.4.4 Port Channel

#### 7.4.4.1 lacp

This command enables Link Aggregation Control Protocol (LACP) on a port group.

**Syntax**

**Lacp <uplinkSetName>**

**no lacp <uplinkSetName>**

**<uplinkSetName> -** The name of a uplink set which the LACP to be enabled or disabled.
**no -** This command disables Link Aggregation Control Protocol (LACP) on a uplink set.

**Default Setting**

Disable

**Command Mode**

Global Config

#### 7.4.4.2 show lacp

This command enables Link Aggregation Control Protocol (LACP) on a uplink set.

**Syntax**

**show lacp [<uplinkSetName>]**

**<uplinkSetName> -** The name of a uplink set which the LACP to be enabled or disabled.

**Default Setting**

Disable

**Command Mode**

Privileged Exec

**Display Message**

**Uplink Set Name:** This indicates the name of uplink set.
**Linkstate:**. This indicates lacp is enabled or disabled for this uplink set

### 7.4.5 Uplink Sets

#### 7.4.5.1 Show Commands

This command display the Uplink Set information.

**Syntax**

**show uplink-set [<uplinkSetName>]**

**<uplinkSetName> -** The name of uplink set which user want to display.

**Default Setting**

None

**Command Mode**

Privileged Exec

**Display Message**

**Uplink Set Name:** This indicates the name of uplink set.
**External Ports:**. The member of the uplink set. The member should be the external ports.
**External Active Ports:** List the external active port members
**External Backup Ports:** List the external backup port members
**Link State:** The status of linkstate for the uplink set.

**Port Backup:** The status of port backup for the uplink set.
**IGMP snooping:** The status of the IGMP snooping for the uplink set.
**LACP:** The status of the LACP for the uplink set.

#### 7.4.5.2 Configuration Commands

##### 7.4.5.2.1 uplink-set

This command is used to create or delete an uplink set.

**Syntax**

**uplink-set <uplinkSetName>**

**no uplink-set <uplinkSetName>**

**<uplinkSetName> -** A string associated with uplink set as a convenience. It can be up to 32 alphanumeric characters, and can not be blank.
**no -** This command deletes an existing uplink set.

**Default Setting**

None

**Command Mode**

Global Config

This command is used to add or remove a port to/form a uplink set.

**Syntax**

**uplink-set <uplinkSetName>**

**no uplink-set <uplinkSetName>**

**<uplinkSetName> -** A string associated with uplink set as a convenience. It can be up to 32 alphanumeric characters, and can not be blank.
**no -** This command remove a port from a uplink set.

**Default Setting**

None

**Command Mode**

Interface Config

### 7.4.6 Port Group

#### 7.4.6.1 Show Commands

This command display the port group information.

**Syntax**

**show port-group [<portGroupName>]**

**<portGroupName> -** The name of a port group which user want to display.

**Default Setting**

None

**Command Mode**

Privileged Exec

**Display Message**

**Port Group Name:** This indicates the name of port group.
**Internal Ports:**. List the internal port members
**Uplink Set Name:** The name of the uplink set.
**External Ports:** List the external ports of the port group.

#### 7.4.6.2 Configuration Commands

##### 7.4.6.2.1 port-group

This command is used to create or delete an port group.

**Syntax**

**port-group <portGroupName>**

**no port-group <portGroupName>**

**<portGroupName> -** A string associated with port group as a convenience. It can be up to 32 alphanumeric characters, and can not be blank.
**no -** This command deletes an existing port group.

**Default Setting**

None

**Command Mode**

Global Config

This command is used to add or remove a port to/form a port group.

**Syntax**

**port-group <portGroupName>**

**no port-group <portGroupName>**

**<portGroupName> -** A string associated with port group as a convenience. It should be an existing port group.
**no -** This command remove a port from a port group.

**Default Setting**

None

**Command Mode**

Interface Config

### 7.4.7 Port Backup

#### 7.4.7.1 Show Commands

This command display the port backup information.

**Syntax**

**show port-backup [ <uplinkSetName> [status] | status ]**

**<uplinkSetName> -** The name of a uplink set which user want to display.

**Default Setting**

None

**Command Mode**

Privileged Exec

**Display Message**

**Uplink Set Name:** This indicates the name of uplink set.
**Port Backup:**. This indicates port-backup is enabled or disabled.
**External Active Ports:** This indicates which ports are in active-port list.
**External Backup Ports:** This indicates which ports are in backup-port list.

### 7.4.7.2 Configuration Commands

#### 7.4.7.2.1 port-backup

This command is used to enable or disable port backup for a uplink set

**Syntax**

**port-backup <uplinkSetName>**

**no port-backup <uplinkSetName>**

**<uplinkSetName> -** A string associated with uplink set as a convenience. It should be an existing uplink set.
**no -** This command disable port backup for an existing port group.

**Default Setting**

None

**Command Mode**

Global Config

This command is used to set the failback time of port backup for a uplink set.

**Syntax**

**port-backup <uplinkSetName> failback-time <value>**

**no port-backup <uplinkSetName> failback-time**

**<uplinkSetName> -** A string associated with uplink set a convenience. It should be an existing uplink set.
**<value> -** Time value is range from 1 to 60 seconds. Default value is 60 seconds.
**no -** This command set the failback time to default value for the specific uplink set.

**Default Setting**

60

**Command Mode**

Global Config

This command is used to move a port from active-port list to backup-port list.

**Syntax**

**port-backup**

**no port-backup**

**no -** This command move the port to active-port list.

*Restriction: users are not allowed to move the last member of active port to backup port.*

**Default Setting**

None

**Command Mode**

Interface Config

### 7.4.8 Link State

#### 7.4.8.1 Show Commands

This command display the linkstate information.

**Syntax**

**show linkstate [<uplinkSetName>]**

**<uplinkSetName> -** The name of a uplink set which user want to display.

**Default Setting**

None

**Command Mode**

Privileged Exec

**Display Message**

**Uplink Set Name:** This indicates the name of uplink set
**Linkstate:**. This indicates linkstate is enabled or disabled for this uplink set.

#### 7.4.8.2 Configuration Commands

##### 7.4.8.2.1 linkstate

This command is used to enable or disable linkstate for a uplink set

**Syntax**

| |
|---|
| **linkstate <uplinkSetName>**<br>**no linkstate <uplinkSetName>** |

**<uplinkSetName> -** A string associated with uplink set as a convenience. It should be an existing uplink set.
**no -** This command disable linkstate for an existing uplink set.

**Default Setting**

None

**Command Mode**

Global Config

### 7.4.9 VLAN Port Groups

#### 7.4.9.1 Show Commands

This command display the vlan group information.

**Syntax**

| |
|---|
| **show vlan-group [<vlanGroupName>]** |

**<vlanGroupName> -** The name of a vlan port group which user want to display.

**Default Setting**

None

**Command Mode**

Privileged Exec

**Display Message**

**VLAN port group name:** This indicates the name of vlan port group
**VLAN ID:** The VLAN Identifier of the VLAN Port Group. The range of the VLAN ID is from 1 to 4094
**Internal Ports:** Internal interface, member of that VLAN Port Group.
**Uplink Set Name:** Specified Uplink Set for the external connection
**External Ports:** External interface, member of the specified Uplink Set.
**Native VLAN:**. Native VLAN feature is support on this VLAN Port Group or not

### 7.4.9.2 Configuration Commands

#### 7.4.9.2.1 vlan-group

This command is used to create or destroy a vlan port group.

**Syntax**

**vlan-group <vlanGroupName> <1-4094> <uplinkSetName>**

**no vlan-group <vlanGroupName>**

**<vlanGroupName> -** A string associated with vlan port group as a convenience.
**<1-4094> -** VLAN ID
**<uplinkSetName> -** which uplink set to be the external connection for this vlan port group.
**no -** This command disable linkstate for an existing vlan port group.

**Default Setting**

None

**Command Mode**

Global Config

This command is used to add/remove a port to/from vlan port group.

**Syntax**

**vlan-group <vlanGroupName>**

**no vlan-group <vlanGroupName>**

**<vlanGroupName> -** A string associated with vlan port group as a convenience.
**no -** This command remove a port from the specified vlan port group.

**Default Setting**

None

**Command Mode**

Interface Config

This command is used to set the native VLAN option for a specific VLAN port group.

**Syntax**

**vlan-group-nativeVLAN <vlanGroupName>**

**no vlan-group-nativeVLAN <vlanGroupName>**

**<vlanGroupName> -** A string associated with vlan port group as a convenience.
**no -** This command set the native VLAN option back to default value..

**Default Setting**

Disable

**Command Mode**

Global Config

### 7.4.10 Service LAN

#### 7.4.10.1 Show Commands

This command display the Service LAN information.

**Syntax**

**show svc-lan [<svcLanName>]**

**<svcLanName> -** The name of Service LAN which user want to display.

**Default Setting**

None

**Command Mode**

Privileged Exec

**Display Message**

**Service LAN name:** This indicates the name of Service LAN
**VLAN ID:** The VLAN Identifier of the Service LAN. The range of the VLAN ID is from 1 to 4094
**Internal Ports:** Internal interface, member of that Service LAN.
**Uplink Set Name:** Specified the Uplink Set for the external connection.
**External Ports:** External interface, member of the specified Uplink Set.

#### 7.4.10.2 Configuration Commands

##### 7.4.10.2.1 svc-lan

This command is used to create or destroy a Service LAN.

**Syntax**

**svc-lan <svcLanName> <1-4094> <uplinkSetName>**

**no svc-lan <svcLanName>**

**<svcLanName> -** A string associated with Service LAN as a convenience.
**<1-4094> -** VLAN ID
**<uplinkSetName> -** which uplink set to be the external connection for this service LAN.

**no -** This command destroy the specified Service LAN.

**Default Setting**

None

**Command Mode**

Global Config

This command is used to add/remove a port to/from Service LAN.

**Syntax**

**svc-lan <svcLanName>**

**no svc-lan <svcLanName>**

**<svcLanName> -** A string associated with Service LAN as a convenience.
**no -** This command remove a port from the specified Service LAN.

**Default Setting**

None

**Command Mode**

Interface Config

### 7.4.11 Service VLAN

#### 7.4.11.1 Show Commands

This command display the Service VLAN information.

**Syntax**

**show svc-vlan [<svcVlanName>]**

**<svcVlanName> -** The name of Service VLAN which user want to display.

**Default Setting**

None

**Command Mode**

Privileged Exec

**Display Message**

**Service VLAN name:** This indicates the name of Service VLAN
**VLAN ID:** The VLAN Identifier of the Service VLAN. The range of the VLAN ID is from 1 to 4094.
**Internal Ports:** Internal interface, member of that Service VLAN.
**Uplink Set Name:** Specified the Uplink Set for the external connection.
**External Ports:** External interface, member of the specified Uplink Set.

#### 7.4.11.2 Configuration Commands

##### 7.4.11.2.1 svc-vlan

This command is used to create or destroy a Service VLAN.

**Syntax**

**svc-vlan <svcVlanName> <1-4094> <uplinkSetName>**

**no svc-vlan <svcVlanName>**

**<svcVlanName> -** A string associated with Service VLAN as a convenience.
**<1-4094> -** VLAN ID
**<uplinkSetName> -** which uplink set to be the external connection for this service VLAN.

**no -** This command destroy the existing Service VLAN.

**Default Setting**

None

**Command Mode**

Global Config

This command is used to add/remove a port to/from Service VLAN.

**Syntax**

**svc-vlan <svcVlanName>**

**no svc-vlan <svcVlanName>**

**<svcVlanName> -** A string associated with Service VLAN as a convenience.
**no -** This command remove a port from the specified Service VLAN.

**Default Setting**

None

**Command Mode**

Interface Config

## 7.5 Management Commands

### 7.5.1 Network Commands

#### 7.5.1.1 show ip interface

This command displays configuration settings associated with the IBP's network interface. The network interface is the logical interface used for in-band connectivity with the IBP via any of the IBP's front panel ports. The configuration parameters associated with the IBP's network interface do not affect the configuration of the front panel ports through which traffic is switched or routed.

**Syntax**

**show ip interface**

**Default Setting**

None

**Command Mode**

Privileged Exec

**Display Message**

**IP Address:** The IP address of the interface. The factory default value is 0.0.0.0
**Subnet Mask:** The IP subnet mask for this interface. The factory default value is 0.0.0.0
**Inband Administration VLAN ID:** Specifies the inband administration VLAN ID.

#### 7.5.1.2 show ip redirects

This command displays IP default gateway for this IBP.

**Syntax**

**show ip redirects**

**Default Setting**

None

**Command Mode**

Privileged Exec

**Display Message**

**IP default gateway:** The default gateway for this IP interface. The factory default value is 0.0.0.0

#### 7.5.1.3 show ip filter

This command displays management IP filter status and all designated management stations.

**Syntax**

**show ip filter**

**Default Setting**

None

**Command Mode**

Privileged Exec

**Display Message**

**Index:** The index of stations.
**IP Address:** The IP address of stations that are allowed to make configuration changes to the IBP.

#### 7.5.1.4 mtu

This command sets the maximum transmission unit (MTU) size (in bytes) for physical and port-channel (LAG) interfaces. For the standard implementation, the range of <1518-9216> is a valid integer between 1518-9216.

**Syntax**

**mtu <1518-9216>**

**no mtu**

**<1518-9216> -** Max frame size (Range: 1518 - 9216).

**no -** This command sets the default maximum transmission unit (MTU) size (in bytes) for the interface.

**Default Setting**

1518

**Command Mode**

Interface Config

#### 7.5.1.5 ip address

This command sets the IP Address, and subnet mask. The IP Address and the gateway must be on the same subnet.

**Syntax**

**ip address <ipaddr> <netmask> [<vlan-id>]**

**no ip address**

**<ipaddr> -** IP address

**<netmask> -** Subnet Mask

**<vlan-id> -** Inband Administration VLAN ID, range is from 1~4094.

**no -** Restore the default IP address and Subnet Mask

**Default Setting**

IP address: 0.0.0.0

Subnet Mask: 0.0.0.0

**Command Mode**

Global Config

**Command Usage**

Once the IP address is set, the VLAN ID's value will be assigned to management VLAN.

#### 7.5.1.6 ip default-gateway

This command sets the IP Address of the default gateway.

**Syntax**

**ip default-gateway <gateway>**

**no ip default-gateway**

**< gateway > -** IP address of the default gateway

**no -** Restore the default IP address of the default gateway

**Default Setting**

IP address: 0.0.0.0

**Command Mode**

Global Config

### 7.5.1.7 ip address protocol

This command specifies the network configuration protocol to be used. If you modify this value, the change is effective immediately.

**Syntax**

**ip address protocol {{bootp | dhcp [<vlanID>]} | none}**

**<bootp> -** Obtains IP address from BOOTP.

**<dhcp> -** Obtains IP address from DHCP.

**<none> -** Obtains IP address by setting configuration.

**<vlanID> -** VLAN ID (Range: 1 – 4094).

**Default Setting**

None

**Command Mode**

Global Config

### 7.5.1.8 ip address mgmt-vlan

This command specifies the network configuration inband administration VLAN ID to be used. If you modify this value, the change is effective immediately.

**Syntax**

**ip address mgmt-vlan <vlanID>**

**<vlanID> -** VLAN ID (Range: 1 – 4094).

**Default Setting**

VLAN ID: 1.

**Command Mode**

Global Config

#### 7.5.1.9 ip filter

This command is used to enable the IP filter function.

**Syntax**

**ip filter**

**no ip filter**

**no –** Disable ip filter.

**Default Setting**

Disabled

**Command Mode**

Global Config

This command is used to set an IP address to be a filter.

**Syntax**

**ip filter <ipaddr>**
**no ip filter <ipaddr>**

**<ipaddr> -** Configure a IP address to be a filter.

**No -** Remove this filter IP address.

**Default Setting**

None

**Command Mode**

Global Config

### 7.5.2 Serial Interface Commands

#### 7.5.2.1 show line console

This command displays serial communication settings for the IBP.

**Syntax**

**show line console**

**Default Setting**

None

**Command Mode**

Privileged Exec

**Display Message**

**Serial Port Login Timeout (minutes):** Specifies the time, in minutes, of inactivity on a Serial port connection, after which the IBP will close the connection. Any numeric value between 0 and 160 is allowed, the factory default is 5. A value of 0 disables the timeout.
**Baud Rate:** The default baud rate at which the serial port will try to connect. The available values are 1200, 2400, 4800, 9600, 19200, 38400, 57600, and 115200 bauds.
**Character Size:** The number of bits in a character. The number of bits is always 8.
**Flow Control:** Whether Hardware Flow-Control is enabled or disabled. Hardware Flow

Control is always disabled.
**Stop Bits:** The number of Stop bits per character. The number of Stop bits is always 1.
**Parity:** The Parity Method used on the Serial Port. The Parity Method is always None.
**Password Threshold:** When the logon attempt threshold is reached on the console port, the system interface becomes silent for a specified amount of time before allowing the next logon attempt. (Use the silent time command to set this interval.) When this threshold is reached for Telnet, the Telnet logon interface closes.
**Silent Time (sec):** Use this command to set the amount of time the management console is inaccessible after the number of unsuccessful logon attempts exceeds the threshold set by the password threshold command.

#### 7.5.2.2 line console

This command is used to enter Line configuration mode

| Syntax |
| --- |
| **line console** |

**Default Setting**

None

**Command Mode**

Global Config

#### 7.5.2.3 baudrate

This command specifies the communication rate of the terminal interface. The supported rates are 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200.

| Syntax |
| --- |
| **baudrate {1200 \| 2400 \| 4800 \| 9600 \| 19200 \| 38400 \| 57600 \| 115200}** |
| **no baudrate** |

**no -** This command sets the communication rate of the terminal interface to **9600**.

**Default Setting**

9600

**Command Mode**

Line Config

#### 7.5.2.4 exec-timeout

This command specifies the maximum connect time (in minutes) without console activity. A value of 0 indicates that a console can be connected indefinitely. The time range is 0 to 160.

**Syntax**

**exec-timeout <0-160>**

**<0-160> -** max connect time (Range: 0 -160).

**no -** This command sets the maximum connect time (in minutes) without console activity to 5.

**Default Setting**

5

**Command Mode**

Line Config

#### 7.5.2.5 password-threshold

This command is used to set the password instruction threshold limiting the number of failed login attempts.

**Syntax**

**password-threshold <0-120>**

**no password-threshold**

**<threshold> -** max threshold (Range: 0 - 120).

**no -** This command sets the maximum value to the default.

**Default Setting**

3

**Command Mode**

Line Config

#### 7.5.2.6 silent-time

This command uses to set the amount of time the management console is inaccessible after the number of unsuccessful logon tries exceeds the threshold value.

**Syntax**

**Silent-time <0-65535>**

**<0-65535> -** silent time (Range: 0 - 65535) in seconds.

**no -** This command sets the maximum value to the default.

**Default Setting**

0

**Command Mode**

Line Config

### 7.5.3 Telnet Session Commands

#### 7.5.3.1 telnet

This command establishes a new outbound telnet connection to a remote host.

**Syntax**

**telnet <host> [port] [debug] [line] [echo]**

**<host> -** A hostname or a valid IP address.

**[port] -** A valid decimal integer in the range of 0 to 65535, where the default value is 23.

**[debug] -** Display current enabled telnet options.

**[line] -** Set the outbound telnet operational mode as 'linemode', where by default, the operational mode is 'character mode'.

**[echo] -** Enable local echo.

**Default Setting**

None

**Command Mode**

Privileged Exec

#### 7.5.3.2 show line vty

This command displays telnet settings.

| Syntax |
| --- |
| **show line vty** |

**Default Setting**

None

**Command Mode**

Privileged Exec

**Display Message**

**Remote Connection Login Timeout (minutes):** This object indicates the number of minutes a remote connection session is allowed to remain inactive before being logged off. A zero means there will be no timeout. May be specified as a number from 0 to 160. The factory default is 5.
**Maximum Number of Remote Connection Sessions:** This object indicates the number of simultaneous remote connection sessions allowed. The factory default is 5.
**Allow New Telnet Sessions:** Indicates that new telnet sessions will not be allowed when set to no. The factory default value is yes.
**Password Threshold:** When the logon attempt threshold is reached on the console port, the system interface becomes silent for a specified amount of time before allowing the next logon attempt. (Use the silent time command to set this interval.) When this threshold is reached for Telnet, the Telnet logon interface closes.

#### 7.5.3.3 line vty

This command is used to enter vty (Telnet) configuration mode.

| Syntax |
| --- |
| **line vty** |

**Default Setting**

None

**Command Mode**

Global Config

#### 7.5.3.4 exec-timeout

This command sets the remote connection session timeout value, in minutes. A session is active as long as the session has been idle for the value set. A value of 0 indicates that a session remains active indefinitely. The time is a decimal value from 0 to 160.

**Note:** Changing the timeout value for active sessions does not become effective until the session is reaccessed. Any keystroke will also activate the new timeout duration.

**Syntax**

**exec-timeout <1-160>**

**no exec-timeout**

**<sec> -** max connect time (Range: 1 -160).

**no -** This command sets the remote connection session timeout value, in minutes, to the default.

**Note:** Changing the timeout value for active sessions does not become effective until the session is reaccessed. Any keystroke will also activate the new timeout duration.

**Default Setting**

5

**Command Mode**

Telnet Config

#### 7.5.3.5 password-threshold

This command is used to set the password instruction threshold limited for the number of failed login attempts.

**Syntax**

**password-threshold <0-120>**
**no password-threshold**

**<threshold> -** max threshold (Range: 0 - 120).

**no -** This command sets the maximum value to the default.

**Default Setting**

3

**Command Mode**

Telnet Config

### 7.5.3.6 maxsessions

This command specifies the maximum number of remote connection sessions that can be established. A value of 0 indicates that no remote connection can be established. The range is 0 to 5.

**Syntax**

**maxsessions <0-5>**
**no maxsessions**

**<0-5> -** max sessions (Range: 0 - 5).

**no -** This command sets the maximum value to be 5.

**Default Setting**

5

**Command Mode**

Telnet Config

### 7.5.3.7 sessions

This command regulates new telnet sessions. If sessions are enabled, new telnet sessions can be established until there are no more sessions available. If sessions are disabled, no new telnet sessions are established. An established session remains active until the session is ended or an abnormal network error ends it.

**Syntax**

**sessions**

**no sessions**

**no -** This command disables telnet sessions. If sessions are disabled, no new telnet sessions are established.

**Default Setting**

Enabled

**Command Mode**

Telnet Config

### 7.5.3.8 telnet sessions

This command regulates new outbound telnet connections. If enabled, new outbound telnet sessions can be established until it reaches the maximum number of simultaneous outbound telnet sessions allowed. If disabled, no new outbound telnet session can be established. An established session remains active until the session is ended or an abnormal network error ends it.

**Syntax**

**telnet sessions**

**no telnet sessions**

**no -** This command disables new outbound telnet connections. If disabled, no new outbound telnet connection can be established.

**Default Setting**

Enabled

**Command Mode**

Global Config

### 7.5.3.9 telnet maxsessions

This command specifies the maximum number of simultaneous outbound telnet sessions. A value of 0 indicates that no outbound telnet session can be established.

**Syntax**

**telnet maxsessions <0-5>**

**no maxsessions**

**<0-5> -** max sessions (Range: 0 - 5).

**no -** This command sets the maximum value to be 5.

**Default Setting**

5

**Command Mode**

Global Config

#### 7.5.3.10 telnet exec-timeout

This command sets the outbound telnet session timeout value in minute.

**Note:** Changing the timeout value for active sessions does not become effective until the session is reaccessed. Any keystroke will also activate the new timeout duration.

**Syntax**

**telnet exec-timeout <1-160>**

**no telnet exec-timeout**

**<1-160> -** max connect time (Range: 1 -160).

**no -** This command sets the remote connection session timeout value, in minutes, to the default.

**Note:** Changing the timeout value for active sessions does not become effective until the session is reaccessed. Any keystroke will also activate the new timeout duration.

**Default Setting**

5

**Command Mode**

Global Config

#### 7.5.3.11 show telnet

This command displays the current outbound telnet settings.

| Syntax |
| --- |
| **show telnet** |

**Default Setting**

None

**Command Mode**

User Exec, Privileged Exec

**Display Message**

**Outbound Telnet Login Timeout (in minutes)** Indicates the number of minutes an outbound telnet session is allowed to remain inactive before being logged off. A value of 0, which is the default, results in no timeout.
**Maximum Number of Outbound Telnet Sessions** Indicates the number of simultaneous outbound telnet connections allowed.
**Allow New Outbound Telnet Sessions** Indicates whether outbound telnet sessions will be allowed.

### 7.5.4 SNMP Server Commands

#### 7.5.4.1 show snmp

This command displays SNMP community information.

Six communities are supported. You can add, change, or delete communities. The IBP does not have to be reset for changes to take effect.

The SNMP agent of the IBP complies with SNMP versions 1, 2c, and 3 (for more about the SNMP specification, see the SNMP RFCs). The SNMP agent sends traps through TCP/IP to an external SNMP manager based on the SNMP configuration (the trap receiver and other

SNMP community parameters).

**Syntax**

**show snmp**

**Default Setting**

None

**Command Mode**

Privileged Exec

**Display Message**

**SNMP Community Name:** The community string to which this entry grants access. A valid entry is a case-sensitive alphanumeric string of up to 16 characters. Each row of this table must contain a unique community name.
**Client IP Address:** An IP address (or portion thereof) from which this device will accept SNMP packets with the associated community. The requesting entity's IP address is ANDed with the Subnet Mask before being compared to the IP Address. Note: that if the Subnet Mask is set to 0.0.0.0, an IP Address of 0.0.0.0 matches all IP addresses. The default value is 0.0.0.0
**Client IP Mask:** A mask to be ANDed with the requesting entity's IP address before comparison with IP Address. If the result matches with the IP Address then the address is an authenticated IP address. For example, if the IP Address = 9.47.128.0 and the corresponding Subnet Mask = 255.255.255.0, a range of incoming IP addresses would match. That is, the incoming IP Address could equal 9.47.128.0 - 9.47.128.255. The default value is 0.0.0.0.
**Access Mode:** The access level for this community string.
**Status:** The status of this community access entry.

### 7.5.4.2 show trapflags

This command displays trap conditions. Configure which traps the IBP should generate by enabling or disabling the trap condition. If a trap condition is enabled and the condition is detected, the IBP's SNMP agent sends the trap to all enabled trap receivers. The IBP does not have to be reset to implement the changes. Cold and warm start traps are always generated and cannot be disabled.

**Syntax**

**show trapflags**

**Default Setting**

None

**Command Mode**

Privileged Exec

**Display Message**

**Authentication Flag:** May be enabled or disabled. The factory default is enabled. Indicates whether authentication failure traps will be sent.
**Link Up/Down Flag:** May be enabled or disabled. The factory default is enabled. Indicates whether link status traps will be sent.
**Multiple Users Flag:** May be enabled or disabled. The factory default is enabled. Indicates whether a trap will be sent when the same user ID is logged into the IBP more than once at the same time (either via telnet or serial port).

### 7.5.4.3 snmp-server sysname

This command sets the name of the IBP. The range for name is from 1 to 31 alphanumeric characters.

**Syntax**

**snmp-server sysname <name>**

**<name> -** Range is from 1 to 31 alphanumeric characters.

**Default Setting**

None

**Command Mode**

Global Config

### 7.5.4.4 snmp-server location

This command sets the physical location of the IBP. The range for name is from 1 to 31 alphanumeric characters.

**Syntax**

**snmp-server location <loc>**

**<loc> -** range is from 1 to 31 alphanumeric characters.

**Default Setting**

None

**Command Mode**

Global Config

#### 7.5.4.5 snmp-server contact

This command sets the organization responsible for the network. The range for contact is from 1 to 31 alphanumeric characters.

**Syntax**

**snmp-server contact <con>**

**<con> -** Range is from 1 to 31 alphanumeric characters.

**Default Setting**

None

**Command Mode**

Global Config

#### 7.5.4.6 snmp-server community

This command adds (and names) a new SNMP community. A community name is a name associated with the IBP and with a set of SNMP managers that manage it with a specified privilege level. The length of the name can be up to 16 case-sensitive characters.

**Note:** Community names in the SNMP community table must be unique. If you make multiple entries using the same community name, the first entry is kept and processed and all duplicate entries are ignored.

**Syntax**

**snmp-server community <name>**

**no snmp-server community <name>**

**<name> -** community name (up to 16 case-sensitive characters).

**no -** This command removes this community name from the table. The name is the community name to be deleted.

### Default Setting

Two default community names: public and private. You can replace these default community names with unique identifiers for each community. The default values for the remaining four community names are blank.

### Command Mode

Global Config

This command activates an SNMP community. If a community is enabled, an SNMP manager associated with this community manages the IBP according to its access right. If the community is disabled, no SNMP requests using this community are accepted. In this case the SNMP manager associated with this community cannot manage the IBP until the Status is changed back to Enable.

**Syntax**

**snmp-server community mode <name>**

**no snmp-server community mode <name>**

**<name> -** community name.

**no -** This command deactivates an SNMP community. If the community is disabled, no SNMP requests using this community are accepted. In this case the SNMP manager associated with this community cannot manage the IBP until the Status is changed back to Enable.

### Default Setting

The default public and private communities are enabled by default. The four undefined communities are disabled by default.

### Command Mode

Global Config

This command sets a client IP mask for an SNMP community. The address is the associated community SNMP packet sending address and is used along with the client IP address value to denote a range of IP addresses from which SNMP clients may use that community to access the device. A value of 255.255.255.255 will allow access from only one station, and will use that machine's IP address for the client IP Address. A value of 0.0.0.0 will allow access from any IP address. The name is the applicable community name.

**Syntax**

**snmp-server community ipmask <ipmask> <name>**

**no snmp-server community ipmask <name>**

**<name> -** community name.

**<ipmask> -** a client IP mask.

**no -** This command sets a client IP mask for an SNMP community to **0.0.0.0**. The name is the applicable community name. The community name may be up to 16 alphanumeric characters.

**Default Setting**

0.0.0.0

**Command Mode**

Global Config

This command restricts access to IBP information. The access mode is read-only (also called public) or read/write (also called private).

**Syntax**

**snmp-server community {ro | rw} <name>**

**<name> -** community name.

**<ro> -** access mode is read-only.

**<rw> -** access mode is read/write.

**Default Setting**

None

**Command Mode**

Global Config

### 7.5.4.7 snmp-server host

This command sets a client IP address for an SNMP community. The address is the associated community SNMP packet sending address and is used along with the client IP mask value to denote a range of IP addresses from which SNMP clients may use that community to access the device. A value of 0.0.0.0 allows access from any IP address. Otherwise, this value is ANDed with the mask to determine the range of allowed client IP addresses. The name is the applicable community name.

**Syntax**

**snmp-server host <ipaddr> <name>**

**no snmp-server host <name>**

**<name> -** community name.

**<ipaddr> -** a client IP address.

**no -** This command sets a client IP address for an SNMP community to **0.0.0.0**. The name is the applicable community name.

**Default Setting**

0.0.0.0

**Command Mode**

Global Config

### 7.5.4.8 snmp-server enable traps

This command enables the Authentication trap.

**Syntax**

**snmp-server enable traps authentication**

**no snmp-server enable traps authentication**

**no -** This command disables the Authentication trap.

**Default Setting**

Enabled

**Command Mode**

Global Config

This command enables Link Up/Down traps for the entire IBP. When enabled, link traps are sent only if the Link Trap flag setting associated with the port is enabled (see ‘snmp trap link-status’ command).

**Syntax**

**snmp-server enable traps linkmode**

**no snmp-server enable traps linkmode**

**no -** This command disables Link Up/Down traps for the entire IBP.

**Default Setting**

Enabled

**Command Mode**

Global Config

This command enables Multiple User traps. When the traps are enabled, a Multiple User Trap is sent when a user logs in to the terminal interface (EIA 232 or telnet) and there is an existing terminal interface session.

**Syntax**

**snmp-server enable traps multiusers**

**no snmp-server enable traps multiusers**

**no -** This command disables Multiple User trap.

**Default Setting**

Enabled

**Command Mode**

Global Config

### 7.5.5 SNMP Trap Commands

#### 7.5.5.1 show snmptrap

This command displays SNMP trap receivers. Trap messages are sent across a network to an SNMP Network Manager. These messages alert the manager to events occurring within the IBP or on the network. Six trap receivers are simultaneously supported.

| Syntax |
| --- |
| **show snmptrap** |

**Default Setting**

None

**Command Mode**

Privileged Exec

**Display Message**

**SNMP Trap Name:** The community string of the SNMP trap packet sent to the trap manager. This may be up to 16 alphanumeric characters. This string is case sensitive.
**IP Address:** The IP address to receive SNMP traps from this device. Enter 4 numbers between 0 and 255 separated by periods.
**SNMP Version:** The trap version to be used by the receiver.
**SNMP v1 –** Uses SNMP v1 to send traps to the receiver
**SNMP v2 –** Uses SNMP v2 to send traps to the receiver
**Status:** A pull down menu that indicates the receiver's status (enabled or disabled) and allows the administrator/user to perform actions on this user entry:
**Enable:** send traps to the receiver
**Disable:** do not send traps to the receiver.
**Delete:** remove the table entry.

### 7.5.5.2 snmp trap link-status

This command enables link status traps by interface.

**Note:** This command is valid only when the Link Up/Down Flag is enabled. See ‘snmpserver enable traps linkmode’ command.

**Syntax**

**snmp trap link-status**

**no snmp trap link-status**

**no -** This command disables link status traps by interface.

**Note:** This command is valid only when the Link Up/Down Flag is enabled. (See ‘snmpserver enable traps linkmode’ command.)

**Default Setting**

Disabled

**Command Mode**

Interface Config

This command enables link status traps for all interfaces.

**Note:** This command is valid only when the Link Up/Down Flag is enabled (See ‘snmpserver enable traps linkmode’ command.)

**Syntax**

**snmp trap link-status all**

**no snmp trap link-status all**

**all -** All interfaces.

**no -** This command disables link status traps for all interfaces.

**Note:** This command is valid only when the Link Up/Down Flag is enabled (see “snmpserver enable traps linkmode”).

**Default Setting**

Disabled

**Command Mode**

Global Config

#### 7.5.5.3 snmptrap <name> <ipaddr>

This command adds an SNMP trap name. The maximum length of the name is 16 case-sensitive alphanumeric characters.

**Syntax**

**snmptrap <name> <ipaddr>**

**no snmptrap <name> <ipaddr>**

**<name> -** SNMP trap name (Range: up to 16 case-sensitive alphanumeric characters).

**<ipaddr> -** an IP address of the trap receiver.

**no -** This command deletes trap receivers for a community.

**Default Setting**

None

**Command Mode**

Global Config

#### 7.5.5.4 snmptrap ipaddr

This command changes the IP address of the trap receiver for the specified community name. The maximum length of name is 16 case-sensitive alphanumeric characters.

**Note:** IP addresses in the SNMP trap receiver table must be unique for the same community name. If you make multiple entries using the same IP address and community name, the first entry is retained and processed. All duplicate entries are ignored.

**Syntax**

**snmptrap ipaddr <name> <ipaddr> <ipaddrnew>**

**<name> -** SNMP trap name.

**<ipaddr> -** an original IP address.

**<ipaddrnew> -** a new IP address.

**Default Setting**

None

**Command Mode**

Global Config

#### 7.5.5.5 snmptrap mode

This command activates or deactivates an SNMP trap. Enabled trap receivers are active (able to receive traps). Disabled trap receivers are inactive (not able to receive traps).

**Syntax**

**snmptrap mode <name> <ipaddr>**

**no snmptrap mode <name> <ipaddr>**

**<name> -** SNMP trap name.

**<ipadd> -** an IP address.

**no -** This command deactivates an SNMP trap. Trap receivers are inactive (not able to receive traps).

**Default Setting**

None

**Command Mode**

Global Config

### 7.5.6 HTTP commands

#### 7.5.6.1 show ip http

This command displays the http settings for the IBP.

**Syntax**

**show ip http**

**Default Setting**

None

**Command Mode**

Privileged Exec

**Display Message**

**HTTP Mode (Unsecure):** This field indicates whether the HTTP mode is enabled or disabled.

**HTTP Port:** This field specifies the port configured for HTTP.

**HTTP Mode (Secure):** This field indicates whether the administrative mode of secure HTTP is enabled or disabled.
**Secure Port:** This field specifies the port configured for SSLT.
**Secure Protocol Level(s):** The protocol level may have the values of SSL3, TSL1, or both SSL3 and TSL1.

### 7.5.6.2 ip javamode

This command specifies whether the IBP should allow access to the Java applet in the header frame of the Web interface. When access is enabled, the Java applet can be viewed from the Web interface. When access is disabled, the user cannot view the Java applet.

**Syntax**

**ip javamode**

**no ip javamode**

**no -** This command disallows access to the Java applet in the header frame of the Web interface. When access is disabled, the user cannot view the Java applet.

**Default Setting**

Enabled

**Command Mode**

Global Config

### 7.5.6.3 ip http port

This command is used to set the http port where port can be 1-65535 and the default is port 80.

**Syntax**

**ip http port <1-65535>**

**no ip http port**

**<1-65535> -** HTTP Port value.

**no -** This command is used to reset the http port to the default value.

**Default Setting**

80

**Command Mode**

Global Config

### 7.5.6.4 ip http server

This command enables access to the IBP through the Web interface. When access is enabled, the user can login to the IBP from the Web interface. When access is disabled, the user cannot login to the IBP's Web server.

Disabling the Web interface takes effect immediately. All interfaces are affected.

**Syntax**

**ip http server**

**no ip http server**

**no -** This command disables access to the IBP through the Web interface. When access is disabled, the user cannot login to the IBP's Web server.

**Default Setting**

Enabled

**Command Mode**

Global Config

### 7.5.6.5 ip http secure-port

This command is used to set the SSLT port where port can be 1-65535 and the default is port 443.

**Syntax**

**ip http secure-port <portid>**

**no ip http secure-port**

**<portid> -** SSLT Port value.

**no -** This command is used to reset the SSLT port to the default value.

**Default Setting**

443

**Command Mode**

Global Config

### 7.5.6.6 ip http secure-server

This command is used to enable the secure socket layer for secure HTTP.

**Syntax**

**ip http secure-server**

**no ip http secure-server**

**no -** This command is used to disable the secure socket layer for secure HTTP.

**Default Setting**

Disabled

**Command Mode**

Global Config

#### 7.5.6.7 ip http secure-protocol

This command is used to set protocol levels (versions). The protocol level can be set to TLS1, SSL3 or to both TLS1 and SSL3.

**Syntax**

**ip http secure-protocol <protocollevel1> [protocollevel2]**

**no ip http secure-protocol <protocollevel1> [protocollevel2]**

**<protocollevel1 - 2> -** The protocol level can be set to TLS1, SSL3 or to both TLS1 and SSL3.

**no -** This command is used to remove protocol levels (versions) for secure HTTP.

**Default Setting**

SSL3 and TLS1

**Command Mode**

Global Config

### 7.5.7 Secure Shell (SSH) Commands

#### 7.5.7.1 show ip ssh

This command displays the SSH settings.

**Syntax**

**show ip ssh**

**Default Setting**

None

**Command Mode**

Privileged Exec

**Display Message**

**Administrative Mode:** This field indicates whether the administrative mode of SSH is enabled or disabled.
**Protocol Levels:** The protocol level may have the values of version 1, version 2, or both versions.
**SSH Sessions Currently Active:** This field specifies the current number of SSH connections.
**Max SSH Sessions Allowed:** The maximum number of inbound SSH sessions allowed on the IBP.
**SSH Timeout:** This field is the inactive timeout value for incoming SSH sessions to the IBP.

### 7.5.7.2 ip ssh

This command is used to enable SSH.

**Syntax**

**ip ssh**
**no ip ssh**

**no -** This command is used to disable SSH.

**Default Setting**

Disabled

**Command Mode**

Global Config

### 7.5.7.3 ip ssh protocol

This command is used to set or remove protocol levels (or versions) for SSH. Either SSH1 (1), SSH2 (2), or both SSH 1 and SSH 2 (1 and 2) can be set.

**Syntax**

**ip ssh protocol <protocollevel1> [protocollevel2]**

**<protocollevel1 - 2> -** The protocol level can be set to SSH1, SSH2 or to both SSH 1 and SSH 2.

**Default Setting**

SSH1 and SSH2

**Command Mode**

Global Config

### 7.5.7.4 ip ssh maxsessions

This command specifies the maximum number of SSH connection sessions that can be established. A value of 0 indicates that no ssh connection can be established. The range is 0 to 5.

**Syntax**

**ip ssh maxsessions <0-5>**

**no ip ssh maxsessions**

**<0-5> -** maximum number of sessions.

**no -** This command sets the maximum number of SSH connection sessions that can be established to the default value.

**Default Setting**

SSH1 and SSH2

**Command Mode**

Global Config

### 7.5.7.5 ip ssh timeout

This command sets the SSH connection session timeout value, in minutes. A session is active as long as the session has been idle for the value set. A value of 0 indicates that a session remains active indefinitely. The time is a decimal value from 0 to 160. Changing the timeout value for active sessions does not become effective until the session is reaccessed. Any keystroke will also activate the new timeout duration.

**Syntax**

**ip ssh timeout <1-160>**

**no ip ssh timeout**

**<1-160> -** timeout interval in seconds.

**no -** This command sets the SSH connection session timeout value, in minutes, to the default. Changing the timeout value for active sessions does not become effective until the session is reaccessed. Any keystroke will also activate the new timeout duration.

**Default Setting**

5

**Command Mode**

Global Config

### 7.5.8 DHCP Client Commands

#### 7.5.8.1 ip dhcp restart

This command is used to initiate a BOOTP or DCHP client request.

**Syntax**

**ip dhcp restart**

**Default Setting**

None

**Command Mode**

Global Config

#### 7.5.8.2 ip dhcp client-identifier

This command is used to specify the DCHP client identifier for this IBP. Use the **no** form to restore to default value.

**Syntax**

**ip dhcp client-identifier {text <text> | hex <hex>}**
**no ip dhcp client-identifier**

**<text> -** A text string. (Range: 1-15 characters).

**<hex> -** The hexadecimal value (00:00:00:00:00:00).

**no -** This command is used to restore to default value.

**Default Setting**

System Burned In MAC Address

**Command Mode**

Global Config

### 7.5.9 LOCK Commands

#### 7.5.9.1 lock

This command locks the http access to the IBP and registers the passed “lock_identifier” with this lock. When the lock is set, the Web-GUI presents a message that access to this IBP is currently not possible, bcause it is managed by another application. Use the **no** form to restore to default value.

**Syntax**

**lock <lock_identifier> [EXCLUSIVE]**

**no lock {<lock_identifier>|ALL}**

**< lock_identifier > -** A alphanumeric string. (Range: 1-32 characters).

**no -** This command is used to restore to default value.

**Default Setting**

None

**Command Mode**

Global Config

#### 7.5.9.2 lock_message

This command allows specification of the displayed message in the Web-GUI of IBP when a lock is set. It must be possible to specify any HTML string. Use “**lock_message default**” to restore default value.

**Syntax**

**lock_message {<message_string>| default}**

**< message_string > -** A specify HTML string. (Range: 1-512 characters).

**lock_message default -** This command is used to restore to default value.

**Default Setting**

**< message_string > :** “This intelligent Blade Panel is currently managed by a Virtual IO Manager. Therefore it is not possible to configure this module by the HTTP user interface.

If you want to remove this lock, this Blade server must not be managed by any Virtual IO Manager. In order to release the lock without using the Virtual IO Manager issue the command "no lock <lock_identifier>" for each lock identifier that is registered."

**Command Mode**

Global Config

#### 7.5.9.3 lock_reset

This command resets the IBP to unlock status, and restore all lock configuration.

**Syntax**

**lock_reset**

**Default Setting**

None

**Command Mode**

Global Config

#### 7.5.9.4 show lock

This command displays the information which contented the lock status and the list of lock identifiers that are registered. And displays the current lock message.

**Syntax**

**show lock**

**Default Setting**

None

**Command Mode**

Privileged Exec

**Display Message**

**Lock Status:** This field indicates the current lock status.
**Lock Message:** This field displays the message in the Web-GUI of the IBP when a lock is set.
**Identifier:** This field specifies the registered "lock_identifier" with this lock.
**State:** The state may have the values of None, Normal, or Exclusive.

## 7.6 System Log Management Commands

### 7.6.1 Show Commands

#### 7.6.1.1 show logging

This command displays logging.

**Syntax**

**Show logging**

**Default Setting**

None

**Command Mode**

Privileged Exec

**Display Message**

**Logging Client Local Port** The port on the collector/relay to which syslog messages are sent
**CLI Command Logging** The mode for CLI command logging.
**Console Logging** The mode for console logging.
**Console Logging Severity Filter** The minimum severity to log to the console log. Messages with an equal or lower numerical severity are logged.
**Buffered Logging** The mode for buffered logging.
**Syslog Logging** The mode for logging to configured syslog hosts. If set to disable logging stops to all syslog hosts.
**Log Messages Received** The number of messages received by the log process. This includes messages that are dropped or ignored
**Log Messages Dropped** The number of messages that could not be processed.
**Log Messages Relayed** The number of messages that are relayed.
**Log Messages Ignored** The number of messages that are ignored.

### 7.6.2 show logging buffered

This command displays the message log maintained by the IBP. The message log contains system trace information.

**Syntax**

**Show logging buffered**

**Default Setting**

None

**Command Mode**

Privileged Exec

**Display Message**

**Message:** The message that has been logged.

**Note:** Message log information is not retained across a system reset.

### 7.6.3 show logging traplog

This command displays the trap log maintained by the IBP.
The trap log contains a maximum of 256 entries that wrap.

| Syntax |
| --- |
| **Show logging traplogs** |

**Default Setting**

None

**Command Mode**

Privileged Exec

**Display Message**

**Number of Traps since last reset:** The number of traps that have occurred since the last reset of this device.
**Trap Log Capacity:** The maximum number of traps that could be stored in the IBP.
**Log:** The sequence number of this trap.
**System Up Time:** The relative time since the last reboot of the IBP at which this trap occurred.
**Trap:** The relevant information of this trap.

***Note:*** *Trap log information is not retained across a IBP reset.*

#### 7.6.3.1 show logging hosts

This command displays all configured logging hosts.

**Syntax**

**Show logging hosts**

**Default Setting**

None

**Command Mode**

Privileged Exec

**Display Message**

**Index (used for deleting)**
**IP Address** IP Address of the configured server.
**Severity** The minimum severity to log to the specified address.
**Port** Server Port Number.This is the port on the local host from which syslog messages are sent.
**Status** The state of logging to configured syslog hosts. If the status is disable, no logging occurs.

### 7.6.4 Configuration Commands

#### 7.6.4.1 logging buffered

This command enables logging to in-memory log where up to 128 logs are kept.

**Syntax**

**logging buffered**

**no logging buffered**

**no -** This command disables logging to in-memory log.

**Default Setting**

None

**Command Mode**

Privileged Exec

This command enables wrapping of in-memory logging when full capacity reached. Otherwise when full capacity is reached, logging stops.

**Syntax**

**logging buffered wrap**

**no logging buffered wrap**

**no -** This command disables wrapping of in-memory logging when full capacity reached.

**Default Setting**

None

**Command Mode**

Privileged Exec

### 7.6.4.2 logging console

This command enables logging to the console.

**Syntax**

**logging console [<severitylevel> | <0-7>]**

**no logging console**

**[<severitylevel> | <0-7>] -** The value is specified as either an integer from 0 to 7 or symbolically through one of the following keywords: emergency (0), alert (1), critical (2), error (3), warning (4), notice (5), informational (6), debug (7).

**no -** This command disables logging to the console.

**Default Setting**

None

**Command Mode**

Privileged Exec

### 7.6.4.3 logging host

This command enables logging to a host where up to eight hosts can be configured.

**Syntax**

**logging host <hostaddress> [ <port>] [[<severitylevel> | <0-7>]]**

**<hostaddress> -** IP address of the log server.

**<port> -** Port number.

**[<severitylevel> | <0-7>] -** The value is specified as either an integer from 0 to 7 or symbolically through one of the following keywords: emergency (0), alert (1), critical (2), error (3), warning (4), notice (5), informational (6), debug (7).

**Default Setting**

None

**Command Mode**

Privileged Exec

This command disables logging to hosts.

**Syntax**

**logging host remove <hostindex>**

**< hostindex > -** Index of the log server.

**Default Setting**

None

**Command Mode**

Privileged Exec

This command reconfigures the IP address of the log server.

**Syntax**

**logging host reconfigure <hostindex> <hostaddress>**

**< hostindex > -** Index of the log server.

**<hostaddress> -** New IP address of the log server.

**Default Setting**

None

**Command Mode**

Privileged Exec

#### 7.6.4.4 logging syslog

This command enables syslog logging.

**Syntax**

**logging syslog**
**no logging syslog**

**no -** Disables syslog logging.

**Default Setting**

None

**Command Mode**

Privileged Exec

This command sets the local port number of the LOG client for logging messages.
.

**Syntax**

**logging syslog port <portid>**
**no logging syslog port**

**no -** Resets the local logging port to the default.

**Default Setting**

None

**Command Mode**

Privileged Exec

### 7.6.4.5 clear logging buffered

This command clears all in-memory log.

**Syntax**

**clear logging buffered**

**Default Setting**

None

**Command Mode**

Privileged Exec

## 7.7 Script Management Commands

### 7.7.1 script apply

This command applies the commands in the configuration script to the IBP. The apply command backs up the running configuration and then starts applying the commands in the script file. Application of the commands stops at the first failure of a command.

**Syntax**

**script apply <scriptname>**

**<scriptname> -** The name of the script to be applied.

**Default Setting**

None

**Command Mode**

Privileged Exec

### 7.7.2 script delete

This command deletes a specified script or all the scripts presented in the IBP.

**Syntax**

**script delete {<scriptname> | all}**

**<scriptname> -** The name of the script to be deleted.

**all -** Delete all scripts presented in the IBP.

**Default Setting**

None

**Command Mode**

Privileged Exec

### 7.7.3 script list

This command lists all scripts present on the IBP as well as the total number of files present.

**Syntax**

**script list**

**Default Setting**

None

**Command Mode**

Privileged Exec

### 7.7.4 script show

This command displays the content of a script file.

**Syntax**

**script show <scriptname>**

**<scriptname> -** Name of the script file.

**Default Setting**

None

**Command Mode**

Privileged Exec

## 7.8 User Account Management Commands

### 7.8.1 Show Commands

#### 7.8.1.1 show users

This command displays the configured user names and their settings. This command is only available for users with readwrite privileges. The SNMPv3 fields will only be displayed if SNMP is available on the system.

| Syntax |
| --- |
| **show users** |

**Default Setting**

None

**Command Mode**

Privileged Exec

**Display Message**

**User Name:** The name the user will use to login using the serial port, Telnet or Web. A new user may be added to the IBP by entering a name in a blank entry. The user name may be up to eight characters, and is not case sensitive. Two users are included as the factory default, admin, and guest.
**User Access Mode:** Shows whether the operator is able to change parameters on the IBP (Read/Write) or is only able to view them (Read Only). As a factory default, admin has Read/Write access and guest has Read Only access. There can only be one Read/Write user and up to five Read Only users.
**SNMPv3 AccessMode:** This field displays the SNMPv3 Access Mode. If the value is set to **Read- Write,** the SNMPv3 user will be able to set and retrieve parameters on the system. If the value is set to **ReadOnly,** the SNMPv3 user will only be able to retrieve parameter information. The SNMPv3 access mode may be different from the CLI and Web access mode.
**SNMPv3 Authentication:** This field displays the authentication protocol to be used for the specified login user.
**SNMPv3 Encryption:** This field displays the encryption protocol to be used for the specified login user.

### 7.8.2 Configuration Commands

#### 7.8.2.1 username

This command adds a new user (account) if space permits. The account <username> can be up to eight characters in length. The name may be comprised of alphanumeric characters as well as the dash ('-') and underscore ('_'). The <username> is not case-sensitive.
Six user names can be defined.

This command changes the password of an existing operator. User password should not be more than eight characters in length. If a user is authorized for authentication or encryption is enabled, the password must be eight alphanumeric characters in length. The username and password are not case-sensitive. When a password is changed, a prompt will ask for the operator's former password. If none, press enter.

**Syntax**

**username <username> {password | nopassword}**

**no username <username>**

**<username> -** is a new user name (Range: up to 8 characters).

**no -** This command removes a user name created before.
**Note:** The admin user account cannot be deleted.

**nopassword -** This command sets the password of an existing operator to blank. When a password is changed, a prompt will ask for the operator's former password. If none, press enter.

**Default Setting**

No password

**Command Mode**

Global Config

### 7.8.2.2 username snmpv3 authentication

This command specifies the authentication protocol to be used for the specified login user. The valid authentication protocols are **none**, **md5** or **sha**. If **md5** or **sha** are specified, the user login password will be used as the snmpv3 authentication password. The <username> is the login user name for which the specified authentication protocol will be used.

**Syntax**

**username snmpv3 authentication <username> {none | md5 | sha}**

**no username snmpv3 authentication <username>**

**<username> -** is the login user name.

**md5 -** md5 authentication method.

**sha -** sha authentication method.

**none -** no use authentication method.

**no -** This command sets the authentication protocol to be used for the specified login user to **none**. The <username> is the login user name for which the specified authentication protocol will be used.

**Default Setting**

No authentication

**Command Mode**

Global Config

### 7.8.2.3 username snmpv3 encryption

This command specifies the encryption protocol and key to be used for the specified login user. The valid encryption protocols are **none** or **des**. The **des** protocol requires a **key**, which can be specified on the command line. The **key** may be up to 16 characters. If the **des** protocol is specified but a key is not provided, the user will be prompted to enter the key. If **none** is specified, a key must not be provided. The <username> is the login user name for which the specified encryption protocol will be used.

**Syntax**

**username snmpv3 encryption <username> {none | des [<key>]}**

**no username snmpv3 encryption <username>**

**<username> -** is the login user name.

**des -** des encryption protocol.

**none -** no encryption protocol.

**no -** This command sets the encryption protocol to **none**. The <username> is the login user name for which the specified encryption protocol will be used.

**Default Setting**

No encryption

**Command Mode**

Global Config

## 7.9 Security Commands

### 7.9.1 Show Commands

#### 7.9.1.1 show users authentication

This command displays all users and all authentication login information. It also displays the authentication login list assigned to the default user.

**Syntax**

**show users authentication**

**Default Setting**

None

**Command Mode**

Privileged Exec

**Display Message**

**User:** This field lists every user that has an authentication login list assigned.
**System Login:** This field displays the authentication login list assigned to the user for system login.
**802.1x:** This field displays the authentication login list assigned to the user for 802.1x port security.

#### 7.9.1.2 show authentication

This command displays the ordered authentication methods for all authentication login lists.

**Syntax**

**show authentication**

**Default Setting**

None

**Command Mode**

Privileged Exec

**Display Message**

**Authentication Login List:** This displays the authentication login listname.
**Method 1:** This displays the first method in the specified authentication login list, if any.
**Method 2:** This displays the second method in the specified authentication login list, if any.
**Method 3:** This displays the third method in the specified authentication login list, if any.

### 7.9.1.3 show authentication users

This command displays information about the users assigned to the specified authentication login list. If the login is assigned to non-configured users, the user “default” will appear in the user column.

**Syntax**

**show authentication users <listname>**

**<listname> -** the authentication login listname.

**Default Setting**

None

**Command Mode**

Privileged Exec

**Display Message**

**User Name:** This field displays the user assigned to the specified authentication login list.
**Component:** This field displays the component (User or 802.1x) for which the authentication login list is assigned.

### 7.9.1.4 show dot1x

This command is used to show the status of the dot1x Administrative mode.

**Syntax**

**show dot1x**

**Default Setting**

None

**Command Mode**

Privileged Exec

**Display Message**

**Administrative mode:** Indicates whether authentication control on the IBP is enabled or disabled.

### 7.9.1.5 show dot1x detail

This command is used to show a summary of the global dot1x configuration and the detailed dot1x configuration for a specified port.

**Syntax**

**show dot1x detail <slot/port>**

**<slot/port> -** is the desired interface number.

**Default Setting**

None

**Command Mode**

Privileged Exec

**Display Message**

**Port:** The interface whose configuration is displayed
**Protocol Version:** The protocol version associated with this port. The only possible value is 1, corresponding to the first version of the dot1x specification.
**PAE Capabilities:** The port access entity (PAE) functionality of this port. Possible values are Authenticator or Supplicant.
**Authenticator PAE State:** Current state of the authenticator PAE state machine. Possible values are Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuthorized, and ForceUnauthorized.
**Backend Authentication State:** Current state of the backend authentication state machine. Possible values are Request, Response, Success, Fail, Timeout, Idle, and Initialize.
**Quiet Period:** The timer used by the authenticator state machine on this port to define periods of time in which it will not attempt to acquire a supplicant. The value is expressed in seconds and will be in the range of 0 to 65535.
**Transmit Period:** The timer used by the authenticator state machine on the specified port to determine when to send an EAPOL EAP Request/Identity frame to the supplicant. The value is expressed in seconds and will be in the range of 1 to 65535.
**Supplicant Timeout:** The timer used by the authenticator state machine on this port to timeout the supplicant. The value is expressed in seconds and will be in the range of 1 to 65535.
**Server Timeout:** The timer used by the authenticator on this port to timeout the authentication server. The value is expressed in seconds and will be in the range of 1 to 65535.
**Maximum Requests:** The maximum number of times the authenticator state machine on

this port will retransmit an EAPOL EAP Request/Identity before timing out the supplicant. The value will be in the range of 1 to 10.
**Reauthentication Period:** The timer used by the authenticator state machine on this port to determine when reauthentication of the supplicant takes place. The value is expressed in seconds and will be in the range of 1 to 65535.
**Reauthentication Enabled:** Indicates if reauthentication is enabled on this port. Possible values are True or False.
**Key Transmission Enabled:** Indicates if the key is transmitted to the supplicant for the specified port. Possible values are True or False.
**Control Direction:** Indicates the control direction for the specified port or ports. Possible values are both or in.

#### 7.9.1.6 show dot1x statistics

This command is used to show a summary of the global dot1x configuration and the dot1x statistics for a specified port.

**Syntax**

**show dot1x statistics <slot/port>**

**<slot/port> -** is the desired interface number.

**Default Setting**

None

**Command Mode**

Privileged Exec

**Display Message**

**Port:** The interface whose statistics are displayed.
**EAPOL Frames Received:** The number of valid EAPOL frames of any type that have been received by this authenticator.
**EAPOL Frames Transmitted:** The number of EAPOL frames of any type that have been transmitted by this authenticator.
**EAPOL Start Frames Received:** The number of EAPOL start frames that have been received by this authenticator.
**EAPOL Logoff Frames Received:** The number of EAPOL logoff frames that have been received by this authenticator.
**Last EAPOL Frame Version:** The protocol version number carried in the most recently received EAPOL frame.
**Last EAPOL Frame Source:** The source MAC address carried in the most recently received EAPOL frame.
**EAP Response/Id Frames Received:** The number of EAP response/identity frames that have been received by this authenticator.

**EAP Response Frames Received:** The number of valid EAP response frames (other than resp/id frames) that have been received by this authenticator.
**EAP Request/Id Frames Transmitted:** The number of EAP request/identity frames that have been transmitted by this authenticator.
**EAP Request Frames Transmitted:** The number of EAP request frames (other than request/identity frames) that have been transmitted by this authenticator.
**Invalid EAPOL Frames Received:** The number of EAPOL frames that have been received by this authenticator in which the frame type is not recognized.
**EAP Length Error Frames Received:** The number of EAPOL frames that have been received by this authenticator in which the frame type is not recognized.

### 7.9.1.7 show dot1x summary

This command is used to show a summary of the global dot1x configuration and summary information of the dot1x configuration for a specified port or all ports.

**Syntax**

**show dot1x summary {<slot/port> | all}**

**<slot/port> -** is the desired interface number.

**all -** All interfaces.

**Default Setting**

None

**Command Mode**

Privileged Exec

**Display Message**

**Interface:** The interface whose configuration is displayed.
**Control Mode:** The configured control mode for this port. Possible values are force-unauthorized / force-authorized / auto.
**Operating Control Mode:** The control mode under which this port is operating. Possible values are authorized / unauthorized.
**Reauthentication Enabled:** Indicates whether re-authentication is enabled on this port.
**Port Status:** Indicates if the key is transmitted to the supplicant for the specified port.

### 7.9.1.8 show dot1x users

This command displays 802.1x port security user information for locally configured users.

**Syntax**

**show dot1x users <slot/port>**

**<slot/port> -** is the desired interface number.

**Default Setting**

None

**Command Mode**

Privileged Exec

**Display Message**

**User:** Users configured locally to have access to the specified port.

#### 7.9.1.9 show radius-servers

This command is used to display items of the configured RADIUS servers.

**Syntax**

**show radius-servers**

**Default Setting**

None

**Command Mode**

Privileged Exec

**Display Message**

**IP Address:** IP Address of the configured RADIUS server
**Port:** The port in use by this server
**Type:** Primary or secondary
**Secret Configured:** Yes / No
**Message Authenticator:** The message authenticator attribute configured for the radius server.

#### 7.9.1.10 show radius

This command is used to display the various RADIUS configuration items for the IBP.

**Syntax**

**show radius**

**Default Setting**

None

**Command Mode**

Privileged Exec

**Display Message**

**Current Server IP Address:** Indicates the configured server currently in use for authentication
**Number of configured servers:** The configured IP address of the authentication server
**Number of retransmits:** The configured value of the maximum number of times a request packet is retransmitted
**Timeout Duration:** The configured timeout value, in seconds, for request re-transmissions
**RADIUS Accounting Mode:** Disable or Enabled

### 7.9.1.11 show radius accounting

This command is used to display the configured RADIUS accounting mode, accounting server, and the statistics for the configured accounting server.

**Syntax**

**show radius accounting [statistics <ipaddr>]**

**<ipaddr> -** is an IP Address.

**Default Setting**

None

**Command Mode**

Privileged Exec

**Display Message**

If the optional token 'statistics <ipaddr>' is not included, then only the accounting mode and the RADIUS accounting server details are displayed.

**RADIUS Accounting Mode:** Enabled or disabled
**IP Address:** The configured IP address of the RADIUS accounting server
**Port:** The port in use by the RADIUS accounting server

**Secret Configured:** Yes or No

If the optional token 'statistics <ipaddr>' is included, the statistics for the configured RADIUS accounting server are displayed. The IP address parameter must match that of a previously configured RADIUS accounting server. The following information regarding the statistics of the RADIUS accounting server is displayed.

**RADIUS Accounting Server IP Address:** IP Address of the configured RADIUS accounting server
**Round Trip Time:** The time interval in centiseconds, between the most recent Accounting-Response and the Accounting-Request that matched it from the RADIUS accounting server.
**Requests:** The number of RADIUS Accounting-Request packets sent to this accounting server. This number does not include retransmissions.
**Retransmission:** The number of RADIUS Accounting-Request packets retransmitted to this RADIUS accounting server.
**Responses:** The number of RADIUS packets received on the accounting port from this server.
**Malformed Responses:** The number of malformed RADIUS Accounting-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators and unknown types are not included as malformed accounting responses.
**Bad Authenticators:** The number of RADIUS Accounting-Response packets containing invalid authenticators received from this accounting server.
**Pending Requests:** The number of RADIUS Accounting-Request packets sent to this server that have not yet timed out or received a response.
**Timeouts:** The number of accounting timeouts to this server.
**Unknown Types:** The number of RADIUS packets of unknown types, which were received from this server on the accounting port.
**Packets Dropped:** The number of RADIUS packets received from this server on the accounting port and dropped for some other reason.

### 7.9.1.12 show radius statistics

This command is used to display the statistics for RADIUS or configured server. To show the configured RADIUS server statistic, the IP Address specified must match that of a previously configured RADIUS server. On execution, the following fields are displayed.

**Syntax**

**show radius statistics [<ipaddr>]**

**<ipaddr> -** is an IP Address.

**Default Setting**

None

**Command Mode**

Privileged Exec

**Display Message**

If an IP address is not specified then only the Invalid Server Addresses field is displayed. Otherwise, the other listed fields are displayed.

**Invalid Server Addresses:** The number of RADIUS Access-Response packets received from unknown addresses.
**Server IP Address:** The IP address of radius server.
**Round Trip Time:** The time interval, in hundredths of a second, between the most recent Access-Reply/ Access-Challenge and the Access-Request that matched it from the RADIUS authentication server.
**Access Requests:** The number of RADIUS Access-Request packets sent to this server. This number does not include retransmissions.
**Access Retransmission:** The number of RADIUS Access-Request packets retransmitted to this RADIUS authentication server.
**Access Accepts:** The number of RADIUS Access-Accept packets, including both valid and invalid packets, which were received from this server.
**Access Rejects:** The number of RADIUS Access-Reject packets, including both valid and invalid packets, which were received from this server.
**Access Challenges:** The number of RADIUS Access-Challenge packets, including both valid and invalid packets, which were received from this server.
**Malformed Access Responses:** The number of malformed RADIUS Access-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators or signature attributes or unknown types are not included as malformed access responses.
**Bad Authenticators:** The number of RADIUS Access-Response packets containing invalid authenticators or signature attributes received from this server.
**Pending Requests:** The number of RADIUS Access-Request packets destined for this server that have not yet timed out or received a response.
**Timeouts:** The number of authentication timeouts to this server.
**Unknown Types:** The number of RADIUS packets of unknown types, which were received from this server on the authentication port.
**Packets Dropped:** The number of RADIUS packets received from this server on the authentication port and dropped for some other reason.

#### 7.9.1.13 show tacacs

This command display configured information of the TACACS.

**Syntax**

**show tacacs**

**Default Setting**

None

**Command Mode**

Privileged Exec

**Display Message**

**Admin Mode:** Displays TACACS administration mode.

**Server 1 Port:** TACACS packet port number

**Server 1 Key:** Secret Key between TACACS server and client

**Server 1 IP:** First TACACS Server IP address

**Server 1 Timeout (sec):** Timeout value in seconds while TACACS server has no response

**Server 1 Retry:** Retry count if TACACS server has no response

**Server 1 Mode:** Current TACACS server admin mode (disable, master or slave)

**Server 2 Port:** TACACS packet port number

**Server 2 Key:** Secret Key between TACACS server and client

**Server 2 IP:** Second TACACS Server IP address

**Server 2 Timeout (sec):** Timeout value in seconds while TACACS server has no response

**Server 2 Retry:** Retry count if TACACS server has no response

**Server 2 Mode:** Current TACACS server admin mode (disable, master or slave)

**Server 3 Port:** TACACS packet port number

**Server 3 Key:** Secret Key between TACACS server and client

**Server 3 IP:** Third TACACS Server IP address

**Server 3 Timeout (sec):** Timeout value in seconds while TACACS server has no response

**Server 3 Retry:** Retry count if TACACS server has no response

**Server 3 Mode:** Current TACACS server admin mode (disable, master or slave)

#### 7.9.1.14 show port-security

This command shows the port-security settings for the entire system.

| Syntax |
| --- |
| **show port-security** |

**Default Setting**

None

**Command Mode**

Privileged Exec

**Display Message**

**Port Security Administration Mode:** Port lock mode for the entire system.

This command shows the port-security settings for a particular interface or all interfaces.

**Syntax**

**show port-security { <slot/port> | all }**

**Default Setting**

None

**Command Mode**

Privileged Exec

**Display Message**

**Intf** Interface Number.
**Interface Admin Mode** Port Locking mode for the Interface.
**Dynamic Limit** Maximum dynamically allocated MAC Addresses.
**Static Limit** Maximum statically allocated MAC Addresses.
**Violation Trap Mode** Whether violation traps are enabled.

This command shows the dynamically locked MAC addresses for port.

**Syntax**

**show port-security dynamic <slot/port>**

**Default Setting**

None

**Command Mode**

Privileged Exec

**Display Message**

**MAC address** Dynamically locked MAC address.

This command shows the statically locked MAC addresses for port.

**Syntax**

**show port-security static <slot/port>**

**Default Setting**

None

**Command Mode**

Privileged Exec

**Display Message**

**MAC address** Statically locked MAC address.

This command displays the source MAC address of the last packet that was discarded on a locked port.

**Syntax**

**show port-security violation <slot/port>**

**Default Setting**

None

**Command Mode**

Privileged Exec

**Display Message**

**MAC address** MAC address of discarded packet on locked ports.

### 7.9.2 Configuration Commands

#### 7.9.2.1 authentication login

This command creates an authentication login list. The <**listname>** is up to 15 alphanumeric characters and is not case sensitive. Up to 10 authentication login lists can be configured on the IBP. When a list is created, the authentication method “local” is set as the first method.

When the optional parameters “method1”, “method 2”, and/or “method 3” are used, an ordered

list of methods are set in the authentication login list. If the authentication login list does not exist, a new authentication login list is first created and then the authentication methods are set in the authentication login list. The maximum number of authentication login methods is three. **The possible method values are local, radius, reject, and tacacs.**

The value of **local** indicates that the user's locally stored ID and password are used for authentication. The value of **radius** indicates that the user's ID and password will be authenticated using the RADIUS server. The value of **reject** indicates that the user is never authenticated. The value of **tacacs** indicates that the user's ID and password will be authenticated using the TACACS.

To authenticate a user, the authentication methods in the user's login will be attempted in order until an authentication attempt succeeds or fails.

Note that the default login list included with the default configuration cannot be changed.

**Syntax**

**authentication login <listname> [<method1>] [<method2>] [<method3>]**

**no authentication login <listname>**

**<listname> -** creates an authentication login list (Range: up to 15 characters).

**<method1 - 3> -** The possible method values are local, radius, reject, and tacacs.

**no -** This command deletes the specified authentication login list. The attempt to delete will fail if any of the following conditions are true:

1. The login list name is invalid or does not match an existing authentication login list
2. The specified authentication login list is assigned to any user or to the nonconfigured user for any component.
3. The login list is the default login list included with the default configuration and was not created using 'config authentication login create'. The default login list cannot be deleted.

**Default Setting**

None

**Command Mode**

Global Config

### 7.9.2.2 username defaultlogin

This command assigns the authentication login list to use for non-configured users when attempting to log in to the system. This setting is overridden by the authentication login list assigned to a specific user if the user is configured locally. If this value is not configured, users will be authenticated using local authentication only.

**Syntax**

**username defaultlogin <listname>**

**<listname> -** an authentication login list.

**Default Setting**

None

**Command Mode**

Global Config

### 7.9.2.3 username login

This command assigns the specified authentication login list to the specified user for system login. The <**username>** must be a configured <**username>** and the **<listname>** must be a configured login list.

If the user is assigned a login list that requires remote authentication, all access to the interface from all CLI, web, and telnet sessions will be blocked until the authentication is complete.

Note that the login list associated with the ‘admin’ user cannot be changed to prevent accidental lockout from the IBP.

**Syntax**

**username login <user> <listname>**

**<user> -** is the login user name.

**<listname> -** an authentication login list.

**Default Setting**

None

**Command Mode**

Global Config

### 7.9.3 Dot1x Configuration Commands

#### 7.9.3.1 dot1x initialize

This command begins the initialization sequence on the specified port. This command is only valid if the control mode for the specified port is 'auto'. If the control mode is not 'auto' an error will be returned.

**Syntax**

**dot1x initialize <slot/port>**

**<slot/port> -** is the desired interface number.

**Default Setting**

None

**Command Mode**

Privileged Exec

#### 7.9.3.2 dot1x default-login

This command assigns the authentication login list to use for non-configured users for 802.1x port security. This setting is over-ridden by the authentication login list assigned to a specific user if the user is configured locally. If this value is not configured, users will be authenticated using local authentication only.

**Syntax**

**dot1x defaultl-login <listname>**

**<listname> -** an authentication login list.

**Default Setting**

None

**Command Mode**

Global Config

### 7.9.3.3 dot1x login

This command assigns the specified authentication login list to the specified user for 802.1x port security. The <user> parameter must be a configured user and the <listname> parameter must be a configured authentication login list.

**Syntax**

**dot1x login <user> <listname>**

**<user> -** is the login user name.

**<listname> -** an authentication login list.

**Default Setting**

None

**Command Mode**

Global Config

### 7.9.3.4 dot1x system-auth-control

This command is used to enable the dot1x authentication support on the IBP. By default, the authentication support is disabled. While disabled, the dot1x configuration is retained and can be changed, but is not activated.

**Syntax**

**dot1x system-auth-control**

**no dot1x system-auth-control**

**no -** This command is used to disable the dot1x authentication support on the IBP.

**Default Setting**

Disabled

**Command Mode**

Global Config

### 7.9.3.5 dot1x user

This command adds the specified user to the list of users with access to the specified port or all ports. The <username> parameter must be a configured user.

**Syntax**

**dot1x user <user> {<slot/port> | all}**

**no dot1x user <user> {<slot/port> | all}**

**<user> -** Is the login user name.

**<slot/port> -** Is the desired interface number.

**all -** All interfaces.

**no -** This command removes the user from the list of users with access to the specified port or all ports.

**Default Setting**

None

**Command Mode**

Global Config

### 7.9.3.6 dot1x port-control

This command sets the authentication mode to be used on all ports. The control mode may be one of the following.
**force-unauthorized:** The authenticator PAE unconditionally sets the controlled port to unauthorized.
**force-authorized:** The authenticator PAE unconditionally sets the controlled port to authorized.
**auto:** The authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator, and the authentication server.

**Syntax**

**dot1x port-control all {auto | force-authorized | force-unauthorized}**

**no dot1x port-control all**

**all -** All interfaces.

**no -** This command sets the authentication mode to be used on all ports to 'auto'.

**Default Setting**

auto

**Command Mode**

Global Config

This command sets the authentication mode to be used on the specified port. The control mode may be one of the following.

**force-unauthorized:** The authenticator PAE unconditionally sets the controlled port to unauthorized.
**force-authorized:** The authenticator PAE unconditionally sets the controlled port to authorized.

**auto:** The authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator, and the authentication server.

**Syntax**

**dot1x port-control {auto | force-authorized | force-unauthorized}**

**no dot1x port-control**

**no -** This command sets the authentication mode to be used on the specified port to 'auto'.

**Default Setting**

auto

**Command Mode**

Interface Config

### 7.9.3.7 dot1x max-req

This command sets the maximum number of times the authenticator state machine on this port will transmit an EAPOL EAP Request/Identity frame before timing out the supplicant. The <1-10> value must be in the range 1 - 10.

**Syntax**

**dot1x max-req <1-10>**

**no dot1x max-req**

**<1-10> -** maximum number of times (Range: 1 – 10).

**no -** This command sets the maximum number of times the authenticator state machine on this port will transmit an EAPOL EAP Request/Identity frame before timing out the supplicant to the default value, that is, 2.

**Default Setting**

2

**Command Mode**

Interface Config

### 7.9.3.8 dot1x re-authentication

This command enables re-authentication of the supplicant for the specified port.

**Syntax**

**dot1x re-authentication**

**no dot1x re-authentication**

**no -** This command disables re-authentication of the supplicant for the specified port.

**Default Setting**

Disabled

**Command Mode**

Interface Config

### 7.9.3.9 dot1x re-reauthenticate

This command begins the re-authentication sequence on the specified port. This command is only valid if the control mode for the specified port is 'auto'. If the control mode is not 'auto' an error will be returned.

**Syntax**

**dot1x re-authenticate <slot/port>**

**<slot/port> -** is the desired interface number.

**Default Setting**

None

**Command Mode**

Privileged Exec

### 7.9.3.10 dot1x timeout

This command sets the value, in seconds, of the timer used by the authenticator state machine on this port. Depending on the token used and the value (in seconds) passed; various timeout configurable parameters are set. The following tokens are supported.

**reauth-period:** Sets the value, in seconds, of the timer used by the authenticator state machine on this port to determine when re-authentication of the supplicant takes place. The reauth-period must be a value in the range 1 - 65535.

**quiet-period:** Sets the value, in seconds, of the timer used by the authenticator state machine on this port to define periods of time in which it will not attempt to acquire a supplicant. The quiet-period must be a value in the range 0 - 65535.

**tx-period:** Sets the value, in seconds, of the timer used by the authenticator state machine on this port to determine when to send an EAPOL EAP Request/Identity frame to the supplicant. The quiet-period must be a value in the range 1 - 65535.

**supp-timeout:** Sets the value, in seconds, of the timer used by the authenticator state machine on this port to timeout the supplicant. The supp-timeout must be a value in the range 1 - 65535.

**server-timeout:** Sets the value, in seconds, of the timer used by the authenticator state machine on this port to timeout the authentication server. The supp-timeout must be a value in the range 1 - 65535.

**Syntax**

**dot1x timeout {quiet-period | reauth-period | server-timeout | supp-timeout | tx-period}**

**<seconds>**

**no dot1x timeout {quiet-period | reauth-period | server-timeout | supp-timeout | tx-period}**

**<seconds> -** Value in the range 0 – 65535.

**no -** This command sets the value, in seconds, of the timer used by the authenticator state machine on this port to the default values. Depending on the token used, the corresponding default values are set.

**Default Setting**

reauth-period: 3600 seconds
quiet-period: 60 seconds
tx-period: 30 seconds
supp-timeout: 30 seconds
server-timeout: 30 seconds

**Command Mode**

Interface Config

### 7.9.4 Radius Configuration Commands

#### 7.9.4.1 radius accounting mode

This command is used to enable the RADIUS accounting function.

**Syntax**

**radius accounting mode**

**no radius accounting mode**

**no -** This command is used to set the RADIUS accounting function to the default value - that is, the RADIUS accounting function is disabled.

**Default Setting**

Disabled

**Command Mode**

Global Config

### 7.9.4.2 radius-server host

This command is used to configure the RADIUS authentication and accounting server.
If the **'auth'** token is used, the command configures the IP address to use to connect to a RADIUS authentication server. Up to 3 servers can be configured per RADIUS client. If the maximum number of configured servers is reached, the command will fail until one of the servers is removed by executing the **no** form of the command. If the optional **<port>** parameter is used, the command will configure the UDP port number to use to connect to the configured RADIUS server. In order to configure the UDP port number, the IP address must match that of a previously configured RADIUS authentication server. The port number must lie between 1 - 65535, with 1812 being the default value.

If the **'acct'** token is used, the command configures the IP address to use for the RADIUS accounting server. Only a single accounting server can be configured. If an accounting server is currently configured, it must be removed from the configuration using the no form of the command before this command succeeds. If the optional **<port>** parameter is used, the command will configure the UDP port to use to connect to the RADIUS accounting server. The IP address specified must match that of a previously configured accounting server. If a port is already configured for the accounting server then the new port will replace the previously configured value. The port must be a value in the range 1 - 65535, with 1813 being the default value.

**Syntax**

**radius-server host {acct | auth} <ipaddr> [port]**

**no radius-server host {acct | auth} <ipaddr>**

**<ipaddr> -** is a IP address.

**[port] -** Port number (Range: 1 – 65535)

**no -** This command is used to remove the configured RADIUS authentication server or the RADIUS accounting server. If the 'auth' token is used, the previously configured RADIUS authentication server is removed from the configuration. Similarly, if the 'acct' token is used, the previously configured RADIUS accounting server is removed from the configuration. The <ipaddr> parameter must match the IP address of the previously configured RADIUS authentication / accounting server.

**Default Setting**

None

**Command Mode**

Global Config

### 7.9.4.3 radius-sever key

This command is used to configure the shared secret between the RADIUS client and the RADIUS accounting / authentication server. Depending on whether the **'auth'** or **'acct'** token is used, the shared secret will be configured for the RADIUS authentication or RADIUS accounting server. The IP address provided must match a previously configured server. When this command is executed, the secret will be prompted. The secret must be an alphanumeric value not exceeding 20 characters.

**Syntax**

**radius-server key {acct | auth} <ipaddr>**

**<ipaddr> -** is a IP address.

**Default Setting**

None

**Command Mode**

Global Config

#### 7.9.4.4 radius-server retransmit

This command sets the maximum number of times a request packet is re-transmitted when no response is received from the RADIUS server. The retries value is an integer in the range of 1 to 15.

**Syntax**

**radius-server retransmit <retries>**

**no radius-server retransmit**

**<retries> -** the maximum number of times (Range: 1 - 15).

**no -** This command sets the maximum number of times a request packet is re-transmitted, when no response is received from the RADIUS server, to the default value, that is, 10.

**Default Setting**

10

**Command Mode**

Global Config

### 7.9.4.5 radius-server timeout

This command sets the timeout value (in seconds) after which a request must be retransmitted to the RADIUS server if no response is received. The timeout value is an integer in the range of 1 to 30.

**Syntax**

**radius-server timeout <seconds>**

**no radius-server timeout**

**<seconds> -** the maximum timeout (Range: 1 - 30).

**no -** This command sets the timeout value (in seconds) after which a request must be retransmitted to the RADIUS server if no response is received, to the default value, that is, 6.

**Default Setting**

6

**Command Mode**

Global Config

### 7.9.4.6 radius-server msgauth

This command enables the message authenticator attribute for a specified server.

**Syntax**

**radius-server msgauth <ipaddr>**

**<ipaddr> -** is a IP address.

**Default Setting**

None

**Command Mode**

Global Config

#### 7.9.4.7 radius-server primary

This command is used to configure the primary RADIUS authentication server for this RADIUS client. The primary server is the one that is used by default for handling RADIUS requests. The remaining configured servers are only used if the primary server cannot be reached. A maximum of three servers can be configured on each client. Only one of these servers can be configured as the primary. If a primary server is already configured prior to this command being executed, the server specified by the IP address specified used in this command will become the new primary server. The IP address must match that of a previously configured RADIUS authentication server.

**Syntax**

**radius-server primary <ipaddr>**

**<ipaddr> -** is a IP address.

**Default Setting**

None

**Command Mode**

Global Config

### 7.9.5 TACACS Configuration Commands

#### 7.9.5.1 tacacs

This command is used to enable /disable the TACACS function.

**Syntax**

**tacacs**

**no tacacs**

**no -** This command is used to disable the TACACS function.

**Default Setting**

Disabled

**Command Mode**

Global Config

#### 7.9.5.2 tacacs mode

This command is used to enable/select/disable the TACACS server administrative mode

**Syntax**

**tacacs mode <1-3> {master | slave}**
**no tacacs mode <1-3>**

**<1-3> -** The valid value of index is 1, 2, and 3.

**no -** This command is used to disable it.

**Default Setting**

Disabled

**Command Mode**

Global Config

#### 7.9.5.3 tacacs server-ip

This command is used to configure the TACACS server IP address.

**Syntax**

**tacacs server-ip <1-3> <ipaddr>**
**no tacacs server-ip <1-3>**

**<ipaddr> -** An IP address.

**<1-3> -** The valid value of index is 1, 2, and 3.

**no -** This command is used to remove the TACACS server IP address.

**Default Setting**

IP 0.0.0.0

**Command Mode**

Global Config

### 7.9.5.4 tacacs port

This command is used to configure the TACACS server's service port.

**Syntax**

**tacacs port <1-3> <1-65535>**

**no tacacs port <1-3>**

**<1-65535> -** service port (Range: 1 to 65535).

**<1-3> -** The valid value of index is 1, 2, and 3.

**no -** This command is used to reset port-id to the default value.

**Default Setting**

49

**Command Mode**

Global Config

### 7.9.5.5 tacacs key

This command is used to configure the TACACS server shared secret key.

**Syntax**

**tacacs key <1-3>**

**no tacacs key <1-3>**

Note that the length of the secret key is up to 32 characters.

**<1-3> -** The valid value of index is 1, 2, and 3.

**no -** This command is used to remove the TACACS server secret key.

**Default Setting**

None

**Command Mode**

Global Config

### 7.9.5.6 tacacs retry

This command is used to configure the TACACS packet retransmit times.

**Syntax**

**tacacs retry <1-3> <1-9>**
**no tacacs retry <1-3>**

**<1-9> -** retry times (Range: 1 to 9).

**<1-3> -** The valid value of index is 1, 2, and 3.

**no -** This command is used to reset retry value to the default value.

**Default Setting**

5

**Command Mode**

Global Config

### 7.9.5.7 tacacs timeout

This command is used to configure the TACACS request timeout of an instance.

**Syntax**

**tacacs timeout <1-3> <1-255>**
**no tacacs timeout <1-3>**

**<1-255> -** max timeout (Range: 1 to 255).

**<1-3> -** The valid value of index is 1, 2, and 3.

**no -** This command is used to reset the timeout value to the default value.

**Default Setting**

3

**Command Mode**

Global Config

### 7.9.6 Port Security Configuration Commands

#### 7.9.6.1 port-security

This command enables port locking at the system level (Global Config) or port level (Interface Config).

| Syntax |
| --- |
| **port-security**<br>**no port-security** |

**Default Setting**

None

**Command Mode**

Global Config, Interface Config

#### 7.9.6.2 port-security max-dynamic

This command sets the maximum of dynamically locked MAC addresses allowed on a specific port.

**Syntax**

**port-security max-dynamic [<0-600>]**

**no port-security max-dynamic**

**no -** This command resets the maximum of dynamically locked MAC addresses allowed on a specific port to its default value.

**Default Setting**

600

**Command Mode**

Interface Config

### 7.9.6.3 port-security max-static

This command sets the maximum number of statically locked MAC addresses allowed on a specific port.

**Syntax**

**port-security max-static [<0-20>]**

**no port-security max-static**

**no -** This command resets the maximum number of statically locked MAC addresses allowed on a specific port to its default value.

**Default Setting**

20

**Command Mode**

Interface Config

### 7.9.6.4 port-security mac-address

This command adds a MAC address to the list of statically locked MAC addresses.

**Syntax**

**port-security mac-address <mac-addr> <1-3965>**

**no port-security mac-address <mac-addr> <1-3965>**

**<1-3965> VLAN ID**

**<mac-addr>**

**no -** This command removes a MAC address from the list of statically locked MAC addresses.

**Default Setting**

None

**Command Mode**

Interface Config

### 7.9.6.5 port-security mac-address move

This command converts dynamically locked MAC addresses to statically locked addresses.

**Syntax**

**port-security mac-address move**

**Default Setting**

None

**Command Mode**

Interface Config

## 7.10 SNTP Commands

### 7.10.1 Show Commands

#### 7.10.1.1 show sntp

This command displays the current time and configuration settings for the SNTP client, and indicates whether the local time has been properly updated.

**Syntax**

**show sntp**

**Default Setting**

None

**Command Mode**

Privileged Exec

**Display Message**

**Last Update Time** Time of last clock update.
**Last Unicast Attempt Time** Time of last transmit query (in unicast mode).
**Last Attempt Status** Status of the last SNTP request (in unicast mode) or unsolicited message (in broadcast mode).
**Broadcast Count** Current number of unsolicited broadcast messages that have been received and processed by the SNTP client since last reboot.
**Time Zone** Time zone configured.

This command displays SNTP client settings.

**Syntax**

**show sntp client**

**Default Setting**

None

**Command Mode**

Privileged Exec

**Display Message**

**Client Supported Modes** Supported SNTP Modes (Broadcast, Unicast, or Multicast).
**SNTP Version** The highest SNTP version the client supports.
**Port** SNTP Client Port
**Client Mode:** Configured SNTP Client Mode.
**Unicast Poll Interval** Poll interval value for SNTP clients in seconds as a power of two.
**Poll Timeout (Seconds)** Poll timeout value in seconds for SNTP clients.
**Poll Retry** Poll retry value for SNTP clients.

This command displays configured SNTP servers and SNTP server settings.

**Syntax**

**show sntp server**

**Default Setting**

None

**Command Mode**

Privileged Exec

**Display Message**

**Server IP Address** IP Address of configured SNTP Server
**Server Type** Address Type of Server.
**Server Stratum** Claimed stratum of the server for the last received valid packet.
**Server Reference ID** Reference clock identifier of the server for the last received valid packet.
**Server Mode** SNTP Server mode.
**Server Max Entries** Total number of SNTP Servers allowed.
**Server Current Entries** Total number of SNTP configured.
*For each configured server:*
**IP Address** IP Address of configured SNTP Server.
**Address Type** Address Type of configured SNTP server.
**Priority** IP priority type of the configured server.
**Version** SNTP Version number of the server. The protocol version used to query the server in unicast mode.
**Port** Server Port Number
**Last Attempt Time** Last server attempt time for the specified server.
**Last Update Status** Last server attempt status for the server.
**Total Unicast Requests** Number of requests to the server.
**Failed Unicast Requests** Number of failed requests from server.

### 7.10.2 Configuration Commands

### 7.10.2.1 sntp broadcast client poll-interval

This command will set the poll interval for SNTP broadcast clients in seconds as a power of two where <poll-interval> can be a value from 6 to 16.

**Syntax**

**sntp broadcast client poll-interval <6-10>**

**no sntp broadcast client poll-interval**

**<6-10> -** The range is 6 to 16.

**no -** This command will reset the poll interval for SNTP broadcast client back to its default value.

**Default Setting**

6

**Command Mode**

Global Config

### 7.10.2.2 sntp client mode

This command will enable Simple Network Time Protocol (SNTP) client mode and optionally setting the mode to either broadcast, multicast, or unicast.

**Syntax**

**sntp client mode [broadcast | unicast]**

**no sntp client mode**

**no -** This command will disable Simple Network Time Protocol (SNTP) client mode.

**Default Setting**

None

**Command Mode**

Global Config

### 7.10.2.3 sntp client port

This command will set the SNTP client port id and polling interval in seconds.

**Syntax**

**sntp client port <portid> [<6-10>]**

**no sntp client port**

**<portid> -** SNTP client port id.
**<6-10> -** Polling interval. It's 2^(value) seconds where value is 6 to 10.
**no -** Resets the SNTP client port id.

**Default Setting**

The default portid is 123.

**Command Mode**

Global Config

### 7.10.2.4 sntp unicast client poll-interval

This command will set the poll interval for SNTP unicast clients in seconds.

**Syntax**

**sntp unicast client poll-interval <6-10>**

**no sntp unicast client poll-interval**

**<6-10> -** Polling interval. It's 2^(value) seconds where value is 6 to 10.
**no -** This command will reset the poll interval for SNTP unicast clients to its default value.

**Default Setting**

The default value is 6.

**Command Mode**

Global Config

### 7.10.2.5 sntp unicast client poll-timeout

This command will set the poll timeout for SNTP unicast clients in seconds.

**Syntax**

**sntp unicast client poll-timeout <poll-timeout>**

**no sntp unicast client poll-timeout**

**< poll-timeout > -** Polling timeout in seconds. The range is 1 to 30.
**no -** This command will reset the poll timeout for SNTP unicast clients to its default value.

**Default Setting**

The default value is 5.

**Command Mode**

Global Config

### 7.10.2.6 sntp unicast client poll-retry

This command will set the poll retry for SNTP unicast clients in seconds.

**Syntax**

**sntp unicast client poll-retry <poll-retry>**

**no sntp unicast client poll-retry**

**< poll-retry> -** Polling retry in seconds. The range is 0 to 10.
**no -** This command will reset the poll retry for SNTP unicast clients to its default value.

**Default Setting**

The default value is 1.

**Command Mode**

Global Config

### 7.10.2.7 sntp server

This command configures an SNTP server (with a maximum of three) where the server address can be an ip address or a domain name and the address type either ipv4 or dns. The optional priority can be a value of 1-3, the version is a value of 1-4, and the port id is a value of 1-65535.

**Syntax**

**sntp server <ipaddress/domain-name> <addresstype> [<1-3> [<version> [<portid>]]]**

**no sntp server remove <ipaddress/domain-name>**

**< ipaddress/domain-name > -** IP address of the SNTP server.
**< addresstype > -** The address type is ipv4 or dns.
**<1-3> -** The range is 1 to 3.
**<version> -** The range is 1 to 4.
**<portid> -** The range is 1 to 65535.
**no -** This command deletes an server from the configured SNTP servers.

**Default Setting**

None.

**Command Mode**

Global Config

### 7.10.2.8 sntp clock timezone

#### 7.10.2.9

This command sets the time zone for the IBP's internal clock.

**Syntax**

**sntp clock timezone <name> <0-12> <0-59> {before-utc | after-utc}**

**<name> -** Name of the time zone, usually an acronym. (Range: 1-15 characters)
**<0-12> -** Number of hours before/after UTC. (Range: 0-12 hours)
**<0-59> -** Number of minutes before/after UTC. (Range: 0-59 minutes)
**before-utc -** Sets the local time zone before (east) of UTC.
**after-utc -** Sets the local time zone after (west) of UTC.

**Default Setting**

Taipei 08:00 After UTC

**Command Mode**

Global Config

## 7.11 System Utilities

### 7.11.1 clear

#### 7.11.1.1 clear arp

This command causes all ARP entries of type dynamic to be removed from the ARP cache.

**Syntax**

**clear arp**

**Default Setting**

None

**Command Mode**

Privileged Exec

#### 7.11.1.2 clear traplog

This command clears the trap log.

**Syntax**

**clear traplog**

**Default Setting**

None

**Command Mode**

Privileged Exec

#### 7.11.1.3 clear eventlog

This command is used to clear the event log, which contains error messages from the system.

**Syntax**

**clear eventlog**

**Default Setting**

None

**Command Mode**

Privileged Exec

#### 7.11.1.4 clear logging buffered

This command is used to clear the message log maintained by the IBP. The message log contains system trace information.

**Syntax**

**clear logging buffered**

**Default Setting**

None

**Command Mode**

Privileged Exec

### 7.11.1.5 clear config

This command resets the configuration to the factory defaults without powering off the IBP. The IBP is automatically reset when this command is processed. You are prompted to confirm that the reset should proceed.

**Syntax**

**clear config**

**Default Setting**

None

**Command Mode**

Privileged Exec

### 7.11.1.6 clear pass

This command resets all user passwords to the factory defaults without powering off the IBP. You are prompted to confirm that the password reset should proceed.

**Syntax**

**clear pass**

**Default Setting**

None

**Command Mode**

Privileged Exec

#### 7.11.1.7 clear mac address table

This command clear all dynamic mac address from the mac address table of IBP.

**Syntax**

**clear mac-addr-table dynamic**

**Default Setting**

None

**Command Mode**

Privileged Exec

#### 7.11.1.8 clear counters

This command clears the stats for a specified <slot/port> or for all the ports or for the entire IBP based upon the argument.

**Syntax**

**clear counters [<slot/port> | all]**

**<slot/port> -** is the desired interface number.

**all -** All interfaces.

**Default Setting**

None

**Command Mode**

Privileged Exec

#### 7.11.1.9 clear port-group

This command resets port group configuration parameters and management VLAN parameters to the factory defaults.

**Syntax**

**clear port-group**

**Default Setting**

None

**Command Mode**

Privileged Exec

#### 7.11.1.10 enable passwd

This command changes Privileged EXEC password.

**Syntax**

**enable passwd**

**Default Setting**

None

**Command Mode**

Global Config.

#### 7.11.1.11 clear igmp snooping

This command clears the tables managed by the IGMP Snooping function and will attempt to delete these entries from the Multicast Forwarding Database.

**Syntax**

**clear igmp snooping**

**Default Setting**

None

**Command Mode**

Privileged Exec

#### 7.11.1.12 clear ip filter

This command is used to clear all ip filter entries.

**Syntax**

**clear ip filter**

**Default Setting**

None

**Command Mode**

Privileged Exec

#### 7.11.1.13 clear dot1x statistics

This command resets the 802.1x statistics for the specified port or for all ports.

**Syntax**

**clear dot1x statistics {all | <slot/port>}**

**<slot/port> -** is the desired interface number.

**all -** All interfaces.

**Default Setting**

None

**Command Mode**

Privileged Exec

#### 7.11.1.14 clear radius statistics

This command is used to clear all RADIUS statistics.

**Syntax**

**clear radius statistics**

**Default Setting**

None

**Command Mode**

Privileged Exec

#### 7.11.1.15 clear tacacs

This command is used to clear TACACS configuration.

**Syntax**

**clear tacacs**

**Default Setting**

None

**Command Mode**

Privileged Exec

### 7.11.2 copy

This command uploads and downloads to/from the IBP. Local URLs can be specified using tftp or xmodem. The following can be specified as the source file for uploading from the IBP: startup config (startup-config), event log (eventlog), message log (msglog) and trap log (traplog). A URL is specified for the destination.

The command can also be used to download the startup config or code image by specifying the source as a URL and destination as startup-config or image respectively.

The command can be used to the save the running config to flash by specifying the source as running-config and the destination as startup-config {*filename*}.

The command can also be used to download ssh key files as sshkey-rsa, sshkey-rsa2, and sshkey-dsa and http secure-server certificates as sslpem-root, sslpem- server, sslpem-dhweak, and sslpem-dhstrong.

Files upload to PC

**Syntax**

**copy startup-config <sourcefilename> <url>**

**copy {errorlog | log | traplog} <url>**

**copy script <sourcefilename> <url>**

**where <url>={xmodem | tftp://ipaddr/path/file}**

**<sourcefilename> -** The filename of a configuration file or a script file.

**<url> -** xmodem or tftp://ipaddr/path/file.

**errorlog -** event Log file.

**log -** message Log file.

**traplog -** trap Log file.

**Default Setting**

None

**Command Mode**

Privileged Exec

Files download from PC to board

**Syntax**

**copy <url> startup-config <destfilename>**

**copy <url> image <destfilename>**

**copy <url> {sshkey-rsa1 | sshkey-rsa2 | sshkey-dsa}**

**copy <url> {sslpem-root | sslpem-server | sslpem-dhweak | sslpem-dhstrong}**

**copy <url> script <destfilename>**

**where <url>={xmodem | tftp://ipaddr/path/file}**

**<destfilename> -** name of the image file or the script file.

**<url> -** xmodem or tftp://ipaddr/path/file.

**sshkey-rsa1 -** SSH RSA1 Key file.

**sshkey-rsa2 -** SSH RSA2 Key file.

**sshkey-dsa -** SSH DSA Key file.

**sslpem-root -** Secure Root PEM file.

**sslpem-server -** Secure Server PEM file.

**sslpem-dhweak -** Secure DH Weak PEM file.

**sslpem-dhstrong -** Secure DH Strong PEM file.

**Default Setting**

None

**Command Mode**

Privileged Exec

Write running configuration file into flash

**Syntax**

**copy running-config startup-config [filename]**

**<filename> -** name of the configuration file.

**Default Setting**

None

**Command Mode**

Privileged Exec

This command upload or download the pre-login banner file

**Syntax**

**copy clibanner <url>**
**copy <url> clibanner**
**no clibanner**

**<url> -** xmodem or tftp://ipaddr/path/file.
**no -** Delete CLI banner.

**Default Setting**

None

**Command Mode**

Privileged Exec

### 7.11.3 delete

This command is used to delete a configuration or image file.

**Syntax**

**delete <filename>**

**<filename> -** name of the configuration or image file.

**Default Setting**

None

**Command Mode**

Privileged Exec

### 7.11.4 dir

This command is used to display a list of files in Flash memory.

**Syntax**

**dir [boot-rom | config | opcode [<filename>] ]**

**<filename> -** name of the configuration or image file.

**boot-rom -** bootrom.

**config -** configuration file.

**opcode -** run time operation code.

**Default Setting**

None

**Command Mode**

Privileged Exec

**Display Message**

| Column Heading | Description |
|---|---|
| date | The date that the file was created. |
| file name | The name of the file. |
| file type | File types: Boot-Rom, Operation Code, and Config file. |
| startup | Shows if this file is used when the system is started. |
| size | The length of the file in bytes. |

### 7.11.5 whichboot

This command is used to display which files were booted when the system powered up.

**Syntax**

**whichboot**

**Default Setting**

None

**Command Mode**

Privileged Exec

### 7.11.6 boot-system

This command is used to specify the file or image used to start up the system.

**Syntax**

**boot-system {boot-rom | config | opcode} <filename>**

**<filename> -** name of the configuration or image file.

**boot-rom -** bootrom.

**config -** configuration file.

**opcode -** run time operation code.

**Default Setting**

None

**Command Mode**

Privileged Exec

### 7.11.7 ping

This command checks if another computer is on the network and listens for connections. To use this command, configure the IBP for network (in-band) connection (as described in the *FASTPATH 2402/ 4802 Hardware User Guide*). The source and target devices must have the ping utility enabled and running on top of TCP/IP. The IBP can be pinged from any IP workstation with which the IBP is connected through the default VLAN (VLAN 1), as long as there is a physical path between the IBP and the workstation. The terminal interface sends, three pings to the target station.

**Syntax**

**ping <host>**

**<host> -** A host name or an IP address.

**Default Setting**

None

**Command Mode**

Privileged Exec

Ping on changing parameter value

**Syntax**

**ping <host> count <0-20000000> [size <32-512>]**

**ping <host> size <32-512> [count <0-20000000>]**

**<ipaddr> -** an IP address.

**<0-20000000> -** number of pings (Range: 0 - 20000000). Note that 0 means infinite.

**<size> -** packet size (Range: 32 - 512).

**Default Setting**

Count = 5

Size = 32

**Command Mode**

Privileged Exec

### 7.11.8 traceroute

This command is used to discover the routes that packets actually take when traveling to their destination through the network on a hop-by-hop basis. <ipaddr> should be a valid IP address. [port] should be a valid decimal integer in the range of 0(zero) to 65535. The default value is 33434. The optional port parameter is the UDP port used as the destination of packets sent as part of the traceroute. This port should be an unused port on the destination system.

**Syntax**

**traceroute <host> [hops <1-255> [waittime <1-255>]]**

**traceroute <host> [waittime <1-255> [hops <1-255>]]**

**<host> -** A host name or an IP address.

**<1-255> -** Time to wait for a response to a probe, in seconds.

**<1-255> -** The maximum time to live used in outgoing probe packets.

**Default Setting**

None

**Command Mode**

Privileged Exec

### 7.11.9 logging cli-command

This command enables the CLI command Logging feature. The Command Logging component enables the IBP to log all Command Line Interface (CLI) commands issued on the system.

**Syntax**

**Logging cli-command**

**Default Setting**

None

**Command Mode**

Global Config

### 7.11.10 calendar set

This command is used to set the system clock.

**Syntax**

**calendar set <mm/dd/yy> <hh:mm:ss>**

**<mm/dd/yy> -** mm is month (range: 1-12), dd is day (range: 1-31), yy is year (range: 2000-2099>

**<hh:mm:ss> -** hh in 24-hour format (Range: 0 - 23), mm is minute (Range: 0 - 59), ss is second (Range: 0 - 59)

**Default Setting**

None

**Command Mode**

Privileged Exec

### 7.11.11 reload

This command resets the IBP without powering it off. Reset means that all network connections are terminated and the boot code executes. The IBP uses the stored configuration to initialize the system. You are prompted to confirm that the reset should proceed. A successful reset is indicated by the LEDs on the IBP.

**Syntax**

**reload**

**Default Setting**

None

**Command Mode**

Privileged Exec

### 7.11.12 configure

This command is used to activate global configuration mode

**Syntax**

**configure**

**Default Setting**

None

**Command Mode**

Privileged Exec

### 7.11.13 disconnect

This command is used to close a telnet session.

**Syntax**

**disconnect {<0-10> | all}**

**<0-11> -** telnet session ID.

**all -** all telnet sessions.

**Default Setting**

None

**Command Mode**

Privileged Exec

### 7.11.14 hostname

This command is used to set the prompt string.

| Syntax |
| --- |
| **hostname <prompt_string>** |

**< prompt_string > -** Prompt string.

**Default Setting**

vty-0

**Command Mode**

Global Config

### 7.11.15 quit

This command is used to exit a CLI session.

| Syntax |
| --- |
| **quit** |

**Default Setting**

None

**Command Mode**

Privileged Exec

## 7.12 DHCP Commands

### 7.12.1 ip dhcp restart

Submit a DHCP client request.

**Syntax**

**ip dhcp restart**

**Default Setting**

None

**Command Mode**

Global Config

### 7.12.2 ip dhcp client-identifier

This commands specifies the DHCP client identifier for the IBP.

**Syntax**

**ip dhcp client-identifier {text <text> | hex <hex>}**

**<text> -** A text string which length is 1 to 15.

**<hex> -** A hex string which format is XX:XX:XX:XX:XX:XX (X is 0-9, A-F).

**Default Setting**

The default value for client-identifier is a text string "FSC".

**Command Mode**

Global Config

# 8 Using SNMP

SNMP (Simple Network Management Protocol) is a communication protocol designed specifically for managing devices or other elements on a network. Equipment commonly managed with SNMP includes switches, routers and host computers. SNMP is typically used to configure these devices for proper operation in a network environment, as well as to monitor them to evaluate performance or detect potential problems.

To access this IBP from a network management station using SNMP, follow these steps:

1. Install an SNMP management application on your host computer.
2. Verify that the management station and IBP are configured to the same IP domain.
3. Configure the community name and access rights for network management access via SNMP.
4. To receive trap messages from the IBP, you must specify the IP address of the trap managers, associated community names, and trap types that the IBP will generate.
5. An SNMP management station can configure and monitor network devices by setting or reading device variables specified in the Management Infor- mation Base (MIB). The key MIB groups supported by this IBP are listed in this appendix.

   To monitor device status or modify system parameters on the IBP from a network management system, you must access the appropriate MIB variables via your SNMP management application.

## 8.1 Supported MIBs

The standard MIBs are listed in the following table.

| Specifications | Public MIB NAME | MIB FIles |
|---|---|---|
| IEEE 802.1x | IEEE8021-PAE-MIB | dot1x.my |
| IEEE 802.3ad | LAG-MIB | dot3ad.my |
| RFC 1213 | RFC1213-MIB | mib-2.my |
| RFC 2011 | IP-MIB | RFC2011 ip-icmp.my |
| RFC 1493 | BRIDGE-MIB | bridge.my |
| RFC 1643 | ETHERLIKE-MIB | etherlike.my |
| RFC 1907 | SNMPv2-MIB | v2-mib.my |
| RFC 2233 | IF-MIB | if.my |
| RFC 2571 | SNMP-FRAMEWORK-MIB | v3-arch.my |
| RFC 2572 | SNMP-MPD-MIB | v3-mpd.my |
| RFC 2573 | SNMP-TARGET-MIB | v3-tgt.my |
| RFC 2574 | SNMP-USER-BASED-SM-MIB | v3-usm.my |
| RFC 2575 | SNMP-VIEW-BASED-ACM-MIB | v3-acm.my |
| RFC 2576 | SNMP-COMMUNITY-MIB | coex.my |
| RFC 2618 | RADIUS-AUTH-CLIENT-MIB | radius_auth_client.my |
| RFC 2620 | RADIUS-ACC-CLIENT-MIB | radius_acc_client.my |
| RFC 2674 | P-BRIDGE-MIB<br>Q-BRIDGE-MIB | pbridge.my<br>vlan.my |
| RFC 2737 | ENTITY-MIB | entity.my |
| RFC 2819 | RMON-MIB | rmon.my |
| RFC 3289 | DIFFSERV-MIB DIFFSERV-DSCP-TC | diffserv.my, diffserv_dscp_tc.my |
| RFC 2787 | VRRP-MIB | vrrp.my |
| RFC 2932 | IANA-RTPROTO-MIB | rtproto.my |
| RFC 2206 | RSVP-MIB | rsvp.my |
| RFC 1724 | RIPv2-MIB | ripv2.my |
| RFC 2668 | MAU-MIB | rfc2668.my |
| RFC 2934 | PIM-MIB | pim.my |
| RFC 1850 | OSPF-TRAP-MIB | ospf_traps.my |
| RFC 1850 | OSPF-MIB | ospf.my |
| RFC 1213 | MPLS-TC-MIB | mpls_tc.my |
| RFC 3813 | MPLS-LSR-MIB | mpls_lsr.my |

| | | |
|---|---|---|
| RFC 3814 | MPLS-FTN-MIB | mpls_ftn.my |
| RFC 2932 | IPMROUTE-STD-MIB | ipmroute.my |
| RFC 1354 | IP-FORWARD-MIB | ipforward.my |
| RFC 2213 | INTEGRATED-SERVICES-MIB | intserv.my |
| RFC 3291 | INET-ADDRESS-MIB | inetaddress.my |
| RFC 2933 and RFC 3019 | MGMD-STD-MIB | igmp.my |
| RFC 1573 | IANAifType-MIB | iftype.my |
| RFC 2677 | IANA-ADDRESS-FAMILY-NUMBERS-MIB | ianaaddr.my |
| | | |

The private enterprise MIB is listed below.

| Private MIB names | MIB files |
|---|---|
| FSC-SWITCH-MIB | lvl7ref.my |
| KEYING-PRIVATE-MIB | fastpath_keying.my |
| OUTBOUNDTELNET-PRIVATE-MIB | fastpath_telnet.my |
| DVMRP-STD-MIB | dvmrp.my |
| MULTICAST-MIB | fastpathmulticast.my |
| MGMT-SECURITY-MIB | fastpath_mgmt_security.my |
| COS-MIB | fastpath_qos_cos.my |
| QOS-MIB | qos.my |
| QOS-ACL-MIB | qos_acl.my |
| QOS-DIFFSERV-EXTENSIONS-MIB | qos_diffserv_extensions.my |
| QOS-DIFFSERV-PRIVATE-MIB | qos_diffserv_private.my |
| ROUTING-MIB | fastpathrouting.my |
| RADIUS-CLIENT-PRIVATE-MIB | radius.my |
| TACACS-MIB | tacacs.my |
| INVENTORY-MIB | fastpathinventory.my |
| LOGGING-MIB | fastpathlogging.my |
| SNTP-CLIENT-MIB | fastpathsntp.my |
| SWITCHING-MIB | fastpathswitching.my |
| FASTPATH-PORTSECURITY-PRIVATE-MIB | fastpath_portsecurity.my |
| SWITCHING-EXTENSION-MIB | switching_extension.my |

## 8.2 Accessing MIB Objects

MIB objects represent features of the IBP that an SNMP application can control and manage. One example is the RFC-2233 IF-MIB group which you can use to get or set the port configuration by reading or writing to different variables in this MIB group. The variables supported by this group are listed in the following table.

### RFC 2233 IF-MIB

| | | |
|---|---|---|
| interfaces | __ | __ |
| ifNumber | No | RO |
| ifMIBObjects | __ | __ |
| ifTableLastChange | YES | RO |
| ifStackLastChange | No | RO |
| ifTable | Index: | ifIndex |
| ifDescr | Yes | RO |
| ifType | Yes | RO |
| ifMtu | Yes | RO |
| ifSpeed | Yes | RO |
| ifPhysAddress | Yes | RO |
| ifAdminStatus | Yes | RW |
| ifOperStatus | Yes | RO |
| ifLastChange | Yes | RO |
| ifInOctets | Yes | RO |
| ifInUcastPkts | Yes | RO |
| ifInNUcastPkts | Yes | RO |
| ifInDiscards | Yes | RO |
| ifInErrors | Yes | RO |
| ifInUnknownProtos | NO | RO |

| | | |
|---|---|---|
| ifOutOctets | Yes | RO |
| ifOutUcastPkts | Yes | RO |
| ifOutNUcastPkts | Yes | RO |
| ifOutDiscards | NO | RO |
| ifOutErrors | Yes | RO |
| ifOutQLen | NO | RO |
| ifSpecific | NO | RO |
| ifXTable | Index: | ifIndex |
| ifName | Yes | RO |
| ifInMulticastPkts | Yes | RO |
| ifInBroadcastPkts | Yes | RO |
| ifOutMulticastPkts | Yes | RO |
| ifOutBroadcastPkts | Yes | RO |
| ifHCInOctets | Yes | RO |
| ifHCInUcastPkts | Yes | RO |
| ifHCInMulticastPkts | Yes | RO |
| ifHCInBroadcastPkts | Yes | RO |
| ifHCOutOctets | Yes | RO |
| ifHCOutUcastPkts | Yes | RO |
| ifHCOutMulticastPkts | Yes | RO |
| ifHCOutBroadcastPkts | Yes | RO |
| ifLinkUpDownTrapEnable | Yes | RW |
| ifHighSpeed | Yes | RO |
| ifPromiscuousMode | Yes | RW |
| ifConnectorPresent | Yes | RO |
| ifAlias | No | RW |
| ifCounterDiscontinuityTime | Yes | RO |

| | | |
|---|---|---|
| ifStackTable | Indicies: | ifStackHigherLayer |
| ifStackLowerLayer | | |
| ifStackStatus | No | RC |
| ifRcvAddressTable | Indicies: | ifIndex |
| ifRcvAddressAddress | | |
| ifRcvAddressStatus | No | RC |
| ifRcvAddressType | No | RC |
| ifTestTable | Index: | ifTestId |
| ifTestStatus | No | RW |
| ifTestType | No | RW |
| ifTestResult | No | RW |
| ifTestCode | No | RO |
| ifTestOwner | No | RW |

## 8.3 Supported Traps

SNMP traps supported include the following items:

| RFC No. | Title |
|---|---|
| RFC 1215 | coldStar warmStart linkDown linkUp authenticationFailure |
| RFC 1493 | newRoot topologyChange |
| RFC 2819 | risingAlarm fallingAlarm |

# 9 Default Settings

## 9.1 The overview system default settings

The default settings for the system module are shown in the following table.

| | | |
|---|---|---|
| **Management** | | |
| | CLI | serial port / telnet / ssh |
| | HTTP | Java Applet / SSL3.0 , TLS 1.0 |
| | SNMP v1/v2c/v3 | Enterprise MIBs / Standard MIBs / RMON |
| **System** | | |
| | Management VLAN | VLAN 1 |
| | WEB Management | HTTP Mode (Unsecure): Enabled<br>HTTP Port: 80 |
| | Traps | Authentication Flag..... Enable<br>Link Up/Down Flag..... Enable<br>Multiple Users Flag..... Enable<br>Spanning Tree Flag..... Enable<br>DVMRP Traps..... Disable<br>OSPF Traps..... Disable<br>PIM Traps..... Disable |
| | SNMP Communities | public : Read Only<br>private : Read/Write |
| | User Name | admin |
| | Password | admin |
| | Serial Port | baud rate 9600 |
| | IP Settings | IP address and netmask: 0.0.0.0 0.0.0.0 on VLAN 1 |
| | Port Status | |
| | Admin Status | enable |
| | Negotiate | enable |
| | Port Speed | port1~10 : 1G<br>port11~16 : 10/100/1G<br>port17~18 : 10G |
| | Duplex Mode | port1~10 : full<br>port11~16 : half / full<br>port17~18 : full |
| | Flow Control | disable |
| | Port Priority | |
| | SSH | Administrative Mode: ..... Disabled<br>Protocol Levels: ..... Versions 1 and 2 |

| | | |
|---|---|---|
| | SSL | HTTP Mode (Secure): Disabled<br>Secure Port: 443<br>Secure Protocol Level(s): TLS1 SSL3 |
| | 802.1X Port Authent. | disable |
| | RADIUS Client | disable |
| | IGMP Snooping | disable |
| | 802.3ad | enable |
| | SNTP Client | disable |
| | TACACS | disable |
| | StormControl | enable |
| | Link State | disable |
| | Port-Backup | disable |
| | SNMP | |

## 9.2 The default settings for all the configuration commands

The default settings for all the configuration commands are shown in the following table.

| **SB9 DEFAULT CONFIG** | | |
|---|---|---|
| **configure mode** | | |
| | Sntp | sntp unicast client poll-interval 6<br>sntp unicast client poll-timeout 5<br>sntp unicast client poll-retry 1<br>sntp broadcast client poll-interval 6<br>sntp client port 123<br>sntp clock timezone Taipei 8 0 before-utc |
| | logging buffered | logging buffered<br>logging buffered wrap<br>no logging console<br>no logging syslog<br>no logging syslog port |

| | | |
|---|---|---|
| | Ip | ip javamode<br>ip dhcp client-identifier text Default<br>(system clear config : ip dhcp client-identifier hex <MAC address>)<br>no ip http secure-server<br>ip http secure-protocol TLS1 SSL3<br>ip http secure-port 443<br>ip http server<br>no ip ssh<br>ip ssh maxsessions 5<br>ip ssh timeout 5 |
| | username | username defaultlogin defaultList |
| | dot1x | no dot1x system-auth-control<br>dot1x default-login defaultList |
| | Radius | no radius accounting mode<br>radius-server retransmit 4<br>radius-server timeout 5 |
| | telnet | telnet sessions<br>telnet exec-timeout 5<br>telnet maxsessions 5 |
| | snmp-server | snmp-server host 0.0.0.0 public<br>snmp-server community ipmask 0.0.0.0 public<br>snmp-server community ro public<br>snmp-server host 0.0.0.0 private<br>snmp-server community ipmask 0.0.0.0 private<br>snmp-server community rw private<br>snmp-server enable traps authentication<br>snmp-server enable traps linkmode<br>snmp-server enable traps multiusers<br>snmp-server enable traps stpmode<br>no snmp-server enable trap ospf<br>no snmp-server enable trap dvmrp<br>no snmp-server enable trap pim |
| | mac-address-table | mac-address-table aging-time 300 |

| | | |
|---|---|---|
| | tacacs | no tacacs<br>tacacs port 1 49<br>no tacacs key 1<br>no tacacs server-ip 1<br>tacacs timeout 1 3<br>tacacs retry 1 5<br>no tacacs mode 1<br>tacacs port 2 49<br>no tacacs key 2<br>no tacacs server-ip 2<br>tacacs timeout 2 3<br>tacacs retry 2 5<br>no tacacs mode 2<br>tacacs port 3 49<br>no tacacs key 3<br>no tacacs server-ip 3<br>tacacs timeout 3 3<br>tacacs retry 3 5<br>no tacacs mode 3 |
| | port-security | no port-security |
| **In-band administration** | | |
| | ip address | ip address protocol none<br>no ip address |
| **line console mode** | | |
| | line console | exec-timeout 5<br>baudrate 9600<br>password-threshold 3<br>silent-time 0 |
| **line vty mode** | | |
| | line vty | sessions<br>exec-timeout 5<br>maxsessions 5<br>password-threshold 3 |
| **router rip mode** | | |
| | router rip | enable<br>distance rip 15<br>split-horizon simple<br>no auto-summary<br>hostroutesaccept<br>no default-information originate<br>no redistribute connected<br>no redistribute static<br>no redistribute ospf |
| **interface mode** | | |
| | negotiate | negotiate |

| | | |
|---|---|---|
| | lacp | no lacp |
| | dot1x | dot1x port-control auto<br>no dot1x re-authentication<br>dot1x timeout quiet-period 60<br>dot1x timeout reauth-period 3600<br>dot1x timeout supp-timeout 30<br>dot1x timeout tx-period 30<br>dot1x timeout server-timeout 30<br>dot1x max-req 2 |
| | storm-control | no storm-control flowcontrol |
| | snmp | snmp trap link-status |
| | port-security | no port-security<br>port-security max-dynamic 600<br>port-security max-static 20 |
| | snmp-server | no snmp-server enable traps violation |
| | encapsulation | encapsulation ethernet |
| | mtu | mtu 1518 |
| | | |
| SSL & SSH key | | |
| | SSH | SSH DSA Key<br>SSH RSA1 Key<br>SSH RSA2 Key |
| | SSL | Secure DH Strong PEM<br>Secure DH Weak PEM<br>Secure Root PEM<br>Secure Server PEM |
| | | |

# 10 Troubleshooting and Tips

If you are having problems connecting to the network, check your network cabling to ensure that the device in question is properly connected to the network. Then refer to verify that the corresponding port on the IBP is functioning properly.

If you are having problems connecting to the management interface, refer to the troubleshooting chart.

## 10.1 Diagnosing IBP Indicators

If you have a connected a device to a port on the IBP, but the Link LED is off, then check the following items:

1. Verify that the IBP and attached device are powered on.
2. Be sure the cable is plugged into both the IBP and corresponding device.
3. Verify that the proper cable type is used and its length does not exceed specified limits.
4. Check the adapter on the attached device and cable connections for possible defects. Replace the defective adapter or cable if necessary.

5. Verify that all system components have been properly installed. If any network cabling appears to be malfunctioning, test it in an alternate environment where you are sure that all the other components are functioning properly.

## 10.2 Accessing the Management Interface

You can access the management interface for the IBP from anywhere within the attached network using Telnet, a Web browser, or any SNMP-based network management software. If you are having trouble accessing the management interface, then refer to the troubleshooting information displayed in the following table.

| Symptom | Action |
|---|---|
| Cannot connect to the IBP using Telnet, Web browser, or SNMP software | • Be sure you have configured the agent with a valid IP address, subnet mask and default gateway.<br>• If you are trying to connect to the agent via the IP address for a tagged VLAN group, your management station must include the appropriate tag in its transmitted frames.<br>• Check that you have a valid network connection to the IBP and that the port you are using has not been disabled.<br>• Check network cabling between the management station and the IBP.<br>• If you cannot connect using Telnet, there may already be four active sessions. Try connecting again at a later time. |
| Cannot access the on-board configuration program via a serial port connection | • Be sure you have set the terminal emulator program to VT100 compatible, 8 data bits, 1 stop bit, no parity, and 19200 bps.<br>• Check that the null-modem serial cable conforms to the pin-out connections provided in the Operating Manual for the server. |
| Forgot or lost the password | • Restore the “Factory_Default_Config.cfg” file with the “boot system” command described on page 134. |